

HP Systems Insight Manager Technical Reference Guide



Manufacturing Part Number: 356920-007

November 2005, Edition 4.0

©Copyright 2003-2005 Hewlett-Packard

Table of Contents

Legal Notices	32
Warranty	32
Restricted Rights Legend	32
Copyright Notice	32
Trademark Notices	32
Release History	33
Introduction	34
Online Help	34
HP SIM Help Categories	34
Product Overview	36
Additional Resources	36
Related Topics	36
Features	36
Related Topics	41
What's New?	41
What's New for HP SIM 5.0?	41
Related Topics	43
Product Architecture	43
Central Management Server	43
Managed Systems	43
System Collections	44
Network Clients	44
Related Topics	44
Assistance	44
Additional Resources	44
Technical Support	45
Related Topics	45
Getting Started	46
Related Procedures	46
Related Topics	46
Signing In	46
Signing into the GUI	47
Signing In Using SSL	48
Logging into the CLI	48
Logging in Directly on the CMS	49
Remotely Using an SSH Client	49
Related Topics	50
Signing Out	50
Signing Out from the Graphical User Interface (GUI)	50
Signing Out from the Command Line Interface (CLI)	50
Related Topics	50
First Time Wizard	50
Related Procedures	51
Related Topics	52
Performing Initial Setup	52
Initial Setup Process	52
Related Topics	53
Navigating the Home Page	53
Graphical User Interface Features	53
Default Home Page Features	54
Related Topics	55

Customizing the Home Page	55
Related Topics	56
Customizing the System Status Panel	56
Related Topics	57
Setting Language Locale	58
Introduction	58
Setting the Web Browser Language or Locale	58
Configuring the Language Settings in Internet Explorer	58
Configuring the Language Settings in Mozilla	58
Configuring the Language or Locale Settings in Windows	59
Configuring Windows XP Language Settings	59
Configuring Windows 2000 Locale Settings	59
Configuring HP-UX and Linux Language Settings	60
Configuring HP SIM	60
CMS Locale	60
Target Locale	61
Using Command Line Interface Commands	62
HP SIM Commands	62
Related Topic	66
Resource Library	66
Related Topics	69
Discovery and Identification	70
Automatic Discovery	70
IP Protocol	70
IPX Protocol	71
Event Based Auto-Discovery	71
Discovery Templates	72
Hosts Files	72
First Discovery	73
Subsequent Discoveries	73
Manual Discovery	73
Options for Adding a Single System	74
Related Procedures	75
Related Topics	75
Configuring Automatic Discovery	76
Related Procedures	77
Related Topics	77
Creating a New Discovery Task	78
Related Procedures	78
Related Topics	79
Editing a Discovery Task	79
Related Procedures	79
Related Topics	79
Disabling or Enabling a Discovery Task	80
Related Procedures	80
Related Topic	80
Deleting a Discovery Task	80
Related Procedures	80
Related Topics	81
Running a Discovery Task	81
Related Procedures	81
Related Topics	81
System Types	81
Configuring Discovery General Settings	84

Related Topics	85
Discovery Filters	85
Related Procedure	86
Related Topic	86
Managing Discovery Templates	86
Related Procedures	86
Related Topic	87
Creating a New Discovery Template File	87
Related Procedures	87
Related Topics	87
Editing a Discovery Template	87
Related Procedures	88
Related Topics	88
Deleting a Discovery Template	88
Related Procedures	89
Related Topics	89
Adding a System Manually	89
Command Line Interface	91
Related Procedure	91
Related Topics	91
Managing Hosts Files	91
Related Procedures	92
Related Topic	92
Creating a New Hosts File	92
Related Procedures	93
Related Topics	93
Editing a Hosts File	94
Related Procedures	94
Related Topics	94
Deleting a Hosts File	94
Related Procedures	95
Related Topics	95
Adding Systems in a Hosts File to the Database	95
Related Procedures	95
Related Topics	95
Creating a Task to Import a Hosts File for HP Systems Insight Manager Integration Task	95
Importing the .dat File	96
Displaying the Systems	96
Exporting Insight Manager (WIN32) Files	96
Related Procedure	96
Hosts File Extensions	97
Default Values	99
Related Procedure	100
Related Topic	100
IP Ranges	100
Related Procedure	100
Related Topic	100
Identification	101
Initial Identification	102
Identify Systems	102
Related Procedure	102
Related Topic	102
Manage System Types	102

Related Procedures	103
Related Topics	103
Navigating the Manage System Types Page	103
System Type	103
Columns	104
Total	104
Available Buttons	104
Related Procedures	104
Related Topics	104
About System Type Manager	104
Why Add or Modify System Identification?	105
Options for Creating a System Type Manager Rule	105
Related Procedures	106
Related Topics	106
Creating a New STM Rule	106
Command Line Interface	109
Related Procedures	109
Related Topics	109
Editing STM Rule	109
Related Procedures	110
Related Topics	110
Deleting STM Rule	110
Related Procedures	110
Related Topics	110
Additional Information for Creating a New STM Rule	111
Adding New DMI Rules (from Windows CMS Only)	111
Adding New SNMP Rules	111
Things You Should Know About DMI Identification	111
Related Procedures	112
Related Topics	113
Users and Authorizations	114
User Configuration Rights	114
Users and Authorizations Tabs	115
Related Procedures	115
Related Topics	115
Users and User Groups	115
Related Procedures	117
Related Topics	117
Creating New Users	117
Command Line Interface	119
Related Procedures	119
Related Topics	119
Creating New User Groups	119
Command Line Interface	121
Related Procedures	121
Related Topics	121
Editing User Accounts and User Groups	121
Command Line Interface	123
Related Procedures	123
Related Topics	124
Deleting User Accounts and User Groups	124
Command Line Interface	125
Related Procedures	125
Related Topics	125

User and User Group Reports	125
Command Line Interface	126
Related Procedures	126
Related Topics	126
Default User Templates	126
Related Topics	126
Toolboxes	127
Related Procedures	127
Related Topics	127
Creating New Toolboxes	128
Command Line Interface	128
Related Procedures	128
Related Topics	129
Editing Toolboxes	129
Command Line Interface	129
Related Procedures	129
Related Topics	130
Deleting Toolboxes	130
Command Line Interface	130
Related Procedures	130
Related Topics	131
Toolbox Report	131
Command Line Interface	131
Related Procedures	132
Related Topics	132
Authorizations	132
Related Procedures	133
Related Topics	133
Creating New Authorizations	133
Command Line Interface	136
Related Procedures	136
Related Topics	136
Updating Authorizations	136
Command Line Interface	137
Related Procedures	137
Related Topics	137
Deleting Authorizations	138
Command Line Interface	138
Related Procedures	138
Related Topics	139
Authorization Report	139
Command Line Interface	139
Related Procedures	140
Related Topics	140
System Groups	140
Managing System Groups from the GUI	140
Managing System Groups from the CLI Using Mxngroup	141
Related Procedures	141
Related Topic	141
Networking and Security	142
Secure Sockets Layer and Certificates	142
Login and Accounts	142
Single Login, Replicate Agent Settings, and Install Software and Firmware	143
Certificates	143

Related Procedures	143
Related Topics	143
About Login	143
Single Login	143
Signing In	144
Login Authentication on Linux and HP-UX	146
Configuring PAM on a Linux System	146
Configuring PAM on an HP-UX System	146
Related Topics	147
About Secure Task Execution	147
Related Topics	147
Configuring the System Link	148
Related Topics	148
Configuring Login Events	148
Related Topics	149
Configuring Browser Timeout Options	149
Related Topics	150
Server Certificates	150
Related Procedures	151
Related Topics	151
Exporting a Server Certificate	151
Related Procedures	151
Related Topics	152
Editing a Server Certificate	152
Related Procedures	153
Related Topics	153
Creating a Server Certificate	153
Related Procedures	155
Related Topic	155
Importing a Server Certificate	155
Related Procedures	156
Related Topics	156
Creating a Certificate Signing Request	156
Related Procedures	157
Related Topics	157
Submitting a Certificate Signing Request	157
Related Procedures	157
Related Topics	157
Importing a CA-Signed Certificate	158
Related Procedures	159
Related Topics	159
Synchronizing Certificates	159
Related Procedures	159
Related Topics	159
Replicating Trusted Certificates	160
Migrating Trusted System Certificates from the Source CMS to the Target CMS	160
Replicating the Trusted Certificates and Trust Mode from the Source CMS to Trusted Managed Systems using the Replicate Agent Settings Feature	161
Related Procedures	162
Related Topic	163
Trusted Certificates	163
Related Procedures	163
Related Topics	163

Importing Trusted Certificates	164
Related Procedures	164
Related Topics	164
Exporting Trusted Certificates	165
Exporting the System Certificate From HP SIM	165
Exporting the System Certificate from the Browser (Microsoft Internet Explorer Only)	165
Related Procedures	166
Related Topics	166
Deleting Trusted Certificates	166
Related Procedures	167
Related Topics	167
Requiring Trusted Certificates	167
Related Procedures	168
Related Topic	168
Setting Up Trust Relationships	168
Setting up the CMS to Trust Managed ProLiant Servers	168
Configuration at the Managed System	169
Setting Up the Managed Server Running System Management Homepage	170
Setting Up the Managed Server Running Management HTTP Server	171
Managing Browser Warning Messages	173
Related Procedures	173
Related Topics	173
Monitoring Systems, Clusters, and Events	174
About Collections	174
Related Procedures	174
Related Topics	175
Navigating the Systems and Events Panel	175
Tree Controls and Customization	176
Overviews	176
Systems	177
Events	178
Related Procedures	178
Related Topics	178
Viewing the System Overview Page	178
Health Status	178
Uncleared Event Status	178
Related Topics	179
Saving Collections	179
Related Procedures	180
Related Topics	180
Customizing System or Cluster Collections	180
Related Procedures	181
Related Topics	181
Creating System or Cluster Collections	181
Command Line Interface	182
Related Procedures	182
Related Topics	183
Editing System or Cluster Collections	183
Command Line Interface	183
Related Procedures	183
Related Topics	184
Deleting System or Cluster Collections	184

Command Line Interface	184
Related Procedures	184
Related Topics	184
Setting Properties for a System or Cluster Collection	185
Command Line Interface	185
Related Procedures	185
Related Topics	186
Customizing Event Collections	186
Command Line Interface	187
Related Procedures	187
Related Topics	187
Creating Event Collections	187
Command Line Interface	188
Related Procedures	188
Related Topics	188
Editing Event Collections	188
Command Line Interface	189
Related Procedures	189
Related Topics	189
Deleting Event Collections	189
Command Line Interface	190
Related Procedures	190
Related Topics	190
Setting Properties for an Event Collection	190
Command Line Interface	191
Related Procedures	191
Related Topics	191
System Table View Page	191
Related Procedures	192
Related Topics	192
Navigating the System Table View Page	192
View Results As	193
System Health Status Legend	193
More System Information	193
System View Columns	193
System Table View Page Buttons	198
Customizing the View	199
Related Procedures	199
Related Topics	199
Navigating the Tree View	199
Expanding the Tree View	200
Selection in the Tree View	200
Tree View Status	201
Available Drilldowns	201
Selection States for Collections	201
Tree View Buttons	201
Related Topics	202
Navigating the Icon View	202
View Results As	203
System Health Status Legend	203
Icon View Buttons	203
Related Topics	204
Navigating the Picture View Page	204
Rack View Page	204

Enclosure View Page	204
Customizing the View	205
Related Topics	205
About Management Processors	205
Related Topics	206
About Racks and Enclosures	206
Related Topics	207
Customizing the System Table View Page	207
Related Procedures	207
Related Topics	208
Deleting Systems from the Database	208
Related Procedures	209
Related Topics	209
Printing a System Collection Report	209
Related Procedures	210
Related Topics	210
System Status Types	210
Related Topic	211
WBEM Operational Status Types	212
Related Topics	214
Software Status Types	214
Related Topic	215
Cluster Table View Page	215
Related Procedures	216
Related Topic	216
Navigating the Cluster Table View Page	216
View As	217
Cluster Status Legend	217
Customizing the View	217
Cluster Collection Columns	217
Buttons	219
Related Procedures	220
Related Topics	220
Customizing the Cluster Table View Page	220
Related Procedures	220
Related Topics	220
Deleting Clusters from the Database	220
Related Procedures	221
Related Topics	221
Printing a Cluster Collection Report	221
Related Procedures	222
Related Topics	222
Event Table View Page	222
Related Procedures	222
Related Topics	222
Navigating the Event Table View Page	223
Event Status Legend	223
Event Details	223
Event Collection Columns	224
Event Management Buttons	225
Customizing the View	226
Related Procedures	226
Related Topics	226
Customizing the Event Table View Page	227

Related Procedures	227
Related Topics	227
Clearing Events from the Collection	227
Related Procedures	228
Related Topics	228
Deleting Events from the Database	228
Related Procedures	228
Related Topics	228
Assigning Events to Users	228
Related Procedures	229
Related Topics	229
Entering Comments on Events	229
Related Procedures	230
Related Topics	230
Printing an Event Collection Report	230
Related Procedures	231
Related Topics	231
Event Severity Types	231
Related Topics	232
Event Details Section	232
Introduction	232
Event Details	232
Related Topics	234
Searching for Systems and Events	234
Related Procedures	234
Related Topics	235
Basic and Advanced Search	235
Basic Search	235
Advanced Search	235
Related Procedures	236
Related Topic	236
Performing a Basic Search	236
Related Procedures	237
Related Topics	237
Performing an Advanced Search for Systems	237
Related Procedures	238
Related Topics	238
Deleting System Search Results	238
Related Procedures	238
Related Topic	239
Printing System Search Results	239
Related Procedures	239
Related Topic	239
Performing an Advanced Search for Events	239
Related Procedures	241
Related Topic	241
Deleting Event Search Results	241
Related Procedures	241
Related Topic	241
Printing Event Search Results	241
Related Procedures	242
Related Topic	242
Performing an Advanced Search for Clusters	242
Related Procedures	243

Related Topics	243
Deleting Cluster Search Results	243
Related Procedures	244
Related Topic	244
Printing Cluster Search Results	244
Related Procedures	244
Related Topic	245
Search Criteria	245
Software/Firmware Criterion	247
Cleared State Criterion	247
Server Role Criterion	248
Assignee Criterion	248
Event Category Criterion	248
Event Type Criterion	248
Memory Range Criterion	249
Related Topic	249
Reference	249
Related Topics	249
Default Public Collections	249
Shared System Collections	249
Shared Event Collections	253
Related Procedures	253
Related Topics	254
Collection Naming Conventions	254
Related Topics	254
Storage Integration	255
Related Topics	255
Storage Integration Using SMI-S	255
About Storage Systems	255
Related Procedures	256
Related Topics	256
Configuring HP Systems Insight Manager with Storage Systems	256
Configuring HP Systems Insight Manager with Storage Systems	256
Related Procedures	256
Related Topic	257
Viewing Storage Systems	257
Viewing Storage System Collections	257
Viewing Individual Storage Systems	257
Related Procedures	257
Related Topics	258
Viewing Storage System Reports	258
Existing Storage System Reports	258
Custom Reports	259
Related Procedures	259
Related Topics	259
Viewing Storage Array Capacity	259
Viewing Storage Capacity for All Arrays	259
Viewing Storage Capacity for a Single Array	259
Related Procedure	259
Related Topics	259
Changes to HP Systems Insight Manager Storage Functionality when HP Storage Essentials is Installed	260
Related Topics	261
Storage Integration Using SNMP	261

Overview	261
Storage Events	262
Storage Inventory Details	262
Related Procedures	263
Related Topics	263
About Storage Discovery Using SNMP	264
Discovery and Identification	264
Related Procedures	264
Related Topic	264
Discovering Storage Using SNMP	264
Related Procedure	265
Related Topics	265
Using HP Systems Insight Manager with SNMP Storage Solutions	265
Viewing a Storage Event	265
Creating a Storage by Type Group	266
Event Collection and Launch	266
Related Procedures	267
Related Topics	268
Managing with Tasks	269
User Privileges	269
Related Procedures	269
Related Topics	270
About Default Polling Tasks	270
Bi Weekly Data Collection	271
Daily Device Identification	271
Hardware Status Polling for non Servers	271
Hardware Status Polling for Servers	272
Hardware Status Polling for Systems no Longer Disabled	272
Initial Data Collection	272
Initial Hardware Status Polling	272
Software Version Status Polling	272
Software Version Status Polling for Systems no Longer Disabled	273
Related Procedures	273
Related Topic	273
Creating a Task	273
Command Line Interface	274
Default Tools	274
Related Topics	276
Navigating the All Scheduled Tasks Page	276
User Privileges	276
Run Now	276
Edit	277
Delete	277
View Task Results	277
Related Topics	277
Scheduling a Task	277
Viewing All Scheduled Tasks	278
Related Procedures	278
Related Topics	278
Running a Scheduled Task	279
Command Line Interface	279
Related Procedures	279
Related Topics	279
Editing a Scheduled Task	279

Related Procedures	280
Related Topics	280
Deleting a Scheduled Task	280
Related Topics	281
Viewing Task Results	281
Viewing Task Results	281
Viewing Task Instance Results	281
Viewing Target Details	282
Viewing a Printable Report	282
Related Procedures	283
Related Topics	283
Printing Reports	283
Related Procedures	283
Related Topics	283
Task Results List	284
Related Topics	285
Stopping a Task	285
Related Procedures	285
Related Topics	285
Deleting Task Results	285
Command Line Interface	286
Related Procedures	286
Related Topic	286
Applying a Time Filter	286
Related Topics	287
Task Status Types	287
Related Topic	287
Tools that Extend Management	288
Related Procedures	289
Related Topics	290
Cluster Monitor	291
Related Topics	292
Configuring Cluster Resource Settings	292
Related Procedure	292
Related Topics	292
Configuring Node Resource Settings	292
Related Procedure	293
Related Topics	293
Cluster Monitor Cluster Tab	293
Related Topics	294
Cluster Monitor Nodes Tab	294
Related Topics	294
Cluster Monitor Network Tab	294
Related Topics	295
Cluster Monitor Resources Tab	295
Related Topics	296
MSCS Status	296
Monitoring MSCS Status	296
Related Topics	296
Cluster Resources Supported by HP Systems Insight Manager	296
Cluster Monitor States	297
Related Topic	297
Cluster Monitor Resources and Associated Settings	298
Related Procedures	298

Related Topics	298
Cluster Monitor Polling Rate	298
Polling Rates	298
Related Procedures	299
Related Topic	299
Cluster Monitor Resource Thresholds	300
Threshold Overview	300
Related Topic	300
Command Line Tools	300
Command Line Interface	301
Related Topics	301
Creating New Command Line Tools	301
Related Procedures	302
Related Topic	302
New Command Line Tool	302
Additional Information	303
Related Procedures	303
Related Topics	303
New Copy a File Tool	303
Additional Information	304
Example of Creating a Copy a File Tool	304
Related Procedures	305
Related Topics	305
New X Window Tool	305
Additional Information	306
Related Procedures	306
Related Topics	306
Command Line Tools Reference	306
Tool Types	306
Parameterized Strings	306
Tool Filtering	308
Version Numbers	312
Other Requirements	312
Document Type Definition	312
Related Procedures	324
Related Topic	324
Examples of Using Parameter Strings in Command Line Tools	325
Related Procedures	326
Related Topics	326
Custom Commands	326
Related Procedures	327
Related Topic	327
Creating a New Custom Command	327
Related Procedure	328
Related Topic	328
Managing Custom Commands	328
New	329
Edit	329
Run Now/Schedule	329
Delete	329
Related Procedure	329
Related Topic	329
Editing a Custom Command	329
Related Procedure	330

Related Topic	331
Environment Variables for Custom Commands	331
Related Procedures	333
Related Topic	333
New Web Launch Tool	333
Additional Information	334
Related Procedures	334
Related Topics	334
Configuring DMI Access	334
Related Procedure	335
Configuring SNMP Access	335
Related Procedure	335
Device Ping	335
Disk Thresholds	336
Setting Disk Thresholds	336
Removing Disk Thresholds	336
Related Procedures	337
Setting Disk Thresholds	337
Related Procedures	337
Related Topic	337
Creating a Task to Delete Disk Thresholds on a Monthly Basis	337
Creating the Task	338
Related Procedures	338
Related Topic	338
License Manager	338
Related Procedures	339
Related Topics	339
About Keys	339
Related Procedures	340
Related Topics	340
Collecting Keys	341
Related Topics	341
Collect Keys Results	341
Related Topics	342
Deploying Keys	342
Related Topics	343
Selecting Keys	343
Related Topics	343
Deploy Key Results	344
Related Topics	345
Managing Keys	345
Related Topics	346
Viewing Key Database Contents	346
Related Topics	347
Adding Keys From a File	347
Related Topics	348
Adding Key Individually	348
Related Topics	349
Viewing Key Details	349
Related Topics	350
System License Information Reporting	350
System License Information Reporting	351
Upgrade Results	351
Related Procedure	352

Related Topics	352
Licensing with ProLiant Essentials Applications	352
Related Topics	353
Management Processor Tools	353
Controlling System Power Options through Management Processors	354
Related Procedure	355
Controlling the System Locator LED through Management Processors	355
Related Procedure	355
Creating New Users on Management Processors	355
Related Procedures	356
Editing Management Processor Users	356
Related Procedures	357
Deleting Management Processor Users	357
Configuring LAN Access on Management Processors	358
Configuring LDAP Settings on Management Processors	358
Executing Internal Control Actions through Management Processors	359
Upgrading Management Processor Firmware	360
Deploying SSH Public Keys to Management Processors	360
Managing MIBs	361
Related Procedures	361
Viewing a MIB	361
Related Procedures	362
Related Topic	362
Editing a MIB	362
Related Procedures	363
Related Topic	363
Compiling a MIB	364
Related Procedures	364
Related Topic	365
Registering a MIB	365
Related Procedures	366
Related Topics	366
Unregistering a MIB	366
Related Procedures	366
Related Topics	366
Installing OpenSSH	366
Related Procedures	367
Deploying OpenSSH to Multiple Systems Using RDP	368
Installing OpenSSH Using RDP	368
Copying the public key from HP SIM to the Target Systems	368
Related Procedures	369
Creating an OpenSSH Task Through the CLI	370
Creating an OpenSSH Task	370
Creating an OpenSSH Task from the Command Line With an XML File	371
Creating an OpenSSH Task from the Command Line Without an XML File	372
Related Procedures	373
PMP Tools	373
Related Topics	374
Removing and Restoring Tools	374
Removing a Tool	374
Restoring a Tool	375
Related Procedures	375
Related Topics	375

Replicate Agent Settings	375
Related Procedure	376
Related Topics	376
Creating a Replicate Agent Settings Task	376
Related Procedure	377
Related Topics	377
Replicate Agent Settings - Reference	377
Determining the Trust Relationship	377
Changing a Trust Relationship	377
Wake on LAN feature	377
Replicate Agent Settings Events	377
Related Procedure	378
Related Topics	378
RPM Package Manager	378
Related Procedures	378
Installing RPM	378
Related Procedures	379
Related Topic	379
Uninstalling RPM	379
Related Procedures	379
Related Topic	379
Querying RPM	379
Related Procedures	380
Related Topic	380
Verifying RPM	380
Related Procedures	380
Related Topic	380
Server Migration Pack	380
SMP Licensing	381
Related Procedures	381
Accessing the Server Migration Pack	381
Related Topic	381
System Management Homepage	381
Related Procedure	382
Related Topic	382
Accessing the System Management Homepage	382
Related Procedures	382
Related Topics	382
System Page	382
Related Topics	383
Identity Tab for Servers	383
System Status	383
More Information	384
Identification	384
Product Description	385
Contact Information	386
Asset Information	386
Management Processor	386
Associations	386
Related Topics	387
Identity Tab for Management Processors	387
System Status	387
Identification	387
Product Description	388

Related Topics	388
Identity Tab for Virtual Machine Hosts	388
Related Topics	389
Identity Tab for Virtual Machine Guests	390
Related Procedures	391
Related Topics	391
Virtual Machine Controls - Launching the Remote Console	391
Related Procedures	392
Related Topics	392
Virtual Machine Controls - Starting the Virtual Machine	392
Related Procedures	393
Related Topics	393
Virtual Machine Controls - Resetting the Virtual Machine	393
Related Procedures	394
Related Topics	394
Virtual Machine Controls - Pausing the Virtual Machine	394
Related Procedures	394
Related Topics	395
Virtual Machine Controls - Stopping the Virtual Machine	395
Related Procedures	395
Related Topics	396
VM Performance Tab for Hosts	396
Related Topics	397
VM Performance Tab for Guests	397
Related Topics	399
Identity Tab for Clusters	399
Health Status	399
Identification	399
Product Description	400
Related Topics	400
Identity Tab for a Complex	400
Health Status	400
Product Description	401
Summary of Components	401
Related Topics	402
Identity Tab for Partitions	402
Identification	402
Product Description	403
Summary of Components	403
Associations	403
Related Topics	403
Identity Tab for a Storage Host	404
Product Description	404
Host Bus Adapters	405
LUNs	406
Related Topics	407
Identity Tab for a Storage Switch	407
Product Description	407
Ports	408
Status Summary	409
Related Topics	409
Identity Tab for a Storage Array	409
Product Description	410
Ports	411

Storage Volumes	412
Capacity Information	413
Related Topics	413
Identity Tab for a Tape Library	413
Product Description	414
Ports	415
Media Access Devices	415
Changer Devices	416
Related Topics	416
Port Types	416
Related Topics	417
Tools & Links Tab	417
System Management Pages	417
System Web Application Pages	417
HP Systems Insight Manager Pages	417
Storage Essentials Pages	418
Related Procedures	418
Related Topic	418
Version Control	418
Related Procedures	419
Related Topics	419
About the Version Control Agent	419
Additional Resources	420
Related Procedures	420
Related Topics	420
About the Version Control Repository Manager	420
Additional Resources	421
Related Procedures	421
Related Topics	421
About Integration	421
Related Procedures	422
Related Topics	422
About Software Repositories	422
Related Procedures	422
Related Topics	423
About Multiple System Management	423
Related Procedures	423
Related Topics	423
Accessing the Version Control Agent	424
Logging into the VCA	424
Related Procedure	425
Related Topics	425
Accessing the Version Control Repository Manager	425
Accessing VCRM from HP SIM	425
Accessing VCRM In-Place	425
Related Procedure	425
Related Topics	425
Version Control Status Icons	426
Version Control Status	426
Related Procedures	428
Related Topics	428
Installing Software and Firmware	428
Firmware Deployment to Switches	429
Related Procedures	429

Related Topics	430
Initial ProLiant Support Pack Install	430
Related Procedure	437
Related Topic	437
Virtual Machine Management Pack	437
Related Procedures	438
Related Topic	438
Deploying the VMM Agent	438
Related Topics	439
Registering VMM	440
Related Procedure	440
Related Topics	440
Unregistering VMM	440
Related Procedure	440
Related Topics	440
Upgrading VMM	441
Related Topics	441
VM Status Types	441
Related Topic	442
WBEM Based Tools	442
Related Topics	442
Property Pages	442
System Fault Management Overview	443
WBEM Providers Overview	444
Available MSA Tools	445
Partner Applications	446
HP Integrity Essentials Plug-ins	446
HP ProLiant Essentials Plug-ins	447
HP Storage Essentials Plug-ins	449
HP Infrastructure Resource Management Plug-ins	449
Related Topics	450
HP Integrity Essentials Overview	450
HP Integrity Essentials for HP-UX 11i	451
Software deployment	451
Configuration management	451
Workload management	451
Remote server management	452
HP Integrity Essentials for Windows	452
Deployment and configuration	452
Remote server management	452
HP Integrity servers with Linux	452
Central administration	452
HP Integrity Essentials for Linux	453
Deployment and Configuration	453
Workload Management	453
Remote server management	453
HP Integrity servers with OpenVMS	453
Central administration	453
HP Integrity Essentials for OpenVMS	453
Configuration Management	453
Workload Management	454
Remote server management	454
Related Topics	454
Event Monitoring Service Overview	454

HP-UX Bastille Overview	455
Features and Benefits	455
GlancePlus Overview	455
Ignite-UX Overview	456
Integrated Lights-Out Overview	456
Partition Manager Overview	457
Security Patch Check Overview	457
HP Serviceguard Manager Overview	458
Related Topics	459
Software Distributor Overview	459
Webmin Overview	459
Workload Manager Overview	460
HP OpenView Storage Data Protector Overview	460
HP OpenView Performance Agent Overview	461
HP OpenView Storage Area Management Overview	461
HP OpenView Storage Management Appliance Overview	462
HP OpenView Storage Operations Manager Overview	463
Process Resource Manager Overview	463
Reasons to Use PRM	464
Accessing Process Resource Manager From HP SIM	464
HP ProLiant Essentials Applications	464
Monitor and Alert	465
Analyze and Control	465
Provision and Patch	465
Recovery and Scale	465
Remote Management	466
Enterprise Management	466
Other HP Management	466
Related Topics	466
Array Configuration Utility Overview	466
HP ProLiant Essentials Automation Manager Overview	467
Related Topics	467
HP BladeSystem Overview	468
HP Client Manager Overview	468
ProLiant Essentials Vulnerability and Patch Management Pack Overview	469
HP Virtual Server Environment Overview	469
Web JetAdmin Overview	470
HP Storage Essentials Overview	470
Related Topics	471
HP StorageWorks Command View XP Overview	471
HP StorageWorks Command View XP Advanced Edition Overview	471
HP StorageWorks Command View SDM Overview	471
HP StorageWorks Command View Tape Library Overview	472
HP StorageWorks EVA Overview	472
HP StorageWorks Modular Storage Array 1000 Overview	473
Reporting	474
HP ProLiant Essentials Performance Management Pack Reporting	474
System Information Reporting	474
Snapshot Comparison	475
Related Procedures	475
Related Topics	475
System Reporting	475
Running an Existing Report in HTML Format	476
Selecting the Sort Order	477

Viewing an Existing Report in XML Format	477
Viewing an Existing Report in CSV Format	477
Printing an Existing Report	477
Command Line Interface	478
Related Procedures	478
Related Topic	478
Adding a Report	478
Adding a New Report	478
Selecting the Sort Order	479
Printing the Report	479
Command Line Interface	479
Related Procedures	480
Related Topic	480
Editing a Report	480
Command Line Interface	481
Related Procedures	481
Related Topic	481
Copying a Report	481
Command Line Interface	482
Related Procedures	482
Related Topic	482
Showing SQL	482
Related Procedures	483
Related Topic	483
Reporting Views	483
Database Views	483
Related Topics	499
Snapshot Comparison Reporting	499
Related Procedures	500
Related Topic	500
PMP Reporting Options	500
Related Topics	501
Administering Systems and Events	502
Events	504
Related Procedures	505
Related Topics	505
About Administering Events	506
Automatic Event Handling	506
Delete Events	507
Event Filter Settings	507
SNMP Trap Settings	507
Status Change Event Settings	507
Related Procedures	508
Related Topics	508
Creating a New Automatic Event Handling Task with Specified Events and System Attributes	508
Creating an automatic event handling task	508
Related Procedures	509
Related Topics	509
Managing Event Handling Tasks	509
Related Procedures	510
Related Topics	510
Creating an Automatic Event Handling Task with Selected Event and System Attributes	510

Related Procedures	513
Related Topics	514
Creating an Automatic Event Handling Task with an Existing Event Collection	514
Related Procedures	516
Related Topics	516
Editing Automatic Event Handling Tasks	517
Related Procedures	517
Related Topics	517
Copying Automatic Event Handling Tasks	517
Related Procedures	517
Related Topics	518
Viewing Task Definitions	518
Related Procedures	518
Related Topics	518
Viewing Event Task Results	519
Related Procedures	519
Related Topics	519
Enabling or Disabling Automatic Event Handling Tasks	519
Related Procedures	520
Related Topics	520
Configuring E-mail Settings	520
Related Procedures	521
Related Topics	521
Configuring Modem Settings	521
Related Procedures	521
Related Topics	522
Clearing Events	522
Related Procedures	522
Related Topics	522
Deleting Events	522
Related Procedures	523
Related Topics	523
Configuring Event Filters	523
Related Procedures	524
Related Topic	524
Configuring SNMP Traps	524
SNMP Trap Fields	525
Related Procedures	525
Related Topics	525
Configuring Status Change Events	526
Related Procedures	526
Related Topics	526
WBEM Indications	526
Related Procedure	527
Related Topics	527
Subscribing to WBEM Indications	527
Related Procedure	527
Related Topics	527
Unsubscribing to WBEM Indications	528
Related Procedure	528
Related Topics	528
Examples of E-mail Pages	528
Example of Standard E-Mail Page	528

Example of Pager/SMS Page	529
Example of HTML Page	529
Related Procedures	530
Related Topics	530
Service Notification Events	530
Configuration and Setup	531
HP SIM Handling of Service Trap Notifications	531
Service Trap Notification Details	531
Service Trap and MIB Type Information	532
Related Procedures	533
Related Topic	533
Examples of Event Tasks	533
Related Procedures	533
Creating a Paging Task Based on E-mail Notification	533
Related Procedures	535
Creating a Task to Delete All Cleared Events	535
Creating the Event Collection	535
Creating and Scheduling the Task	536
Related Procedures	536
Related Topic	537
Creating a Task to Delete Events Older than Thirty Days	537
Creating the Collection	537
Scheduling the Task	538
Related Procedures	538
Related Topic	538
Creating a Task to Send an E-mail When a System Reaches a Critical State	538
Creating the Collection	539
Configuring HP SIM to Send E-mail	539
Configuring Status Change Events	539
Creating the Task	540
Related Procedures	541
Status Polling	541
Related Procedures	542
Related Topic	542
Software Status Polling	542
Related Procedure	542
Related Topics	542
Hardware Status Polling	543
Related Procedure	544
Related Topics	544
WMI Mapper Proxy	544
Related Procedures	544
Related Topic	545
Adding a WMI Mapper Proxy	545
Related Procedures	545
Related Topic	545
Editing a WMI Mapper Proxy	545
Related Procedures	546
Related Topic	546
Deleting a WMI Mapper Proxy	546
Related Procedures	547
Related Topic	547
Protocols	547
Related Procedures	547

Related Topics	547
Setting Global Protocols	548
Related Topics	550
Setting Protocols for a System or Groups of Systems	550
Related Procedures	551
Related Topics	551
Setting Protocols for a Single System	551
Related Procedures	553
Related Topics	553
Global Protocols	553
SNMP	553
DMI	554
HTTP	555
WBEM	555
Related Procedures	555
Related Topics	555
Data Collection	555
Append New Data Set (for Historical Trend Analysis)	557
Overwrite Existing Data Set (for Detailed Analysis)	557
Initial Data Collection	558
Bi-Weekly Data Collection	558
Related Procedure	558
Related Topics	558
Creating a Data Collection Task	558
Command Line Interface	559
Related Topics	559
System Properties	559
Related Procedures	560
Related Topics	560
Editing System Properties for a Single System	560
Related Procedure	562
Related Topics	562
Editing System Properties for Multiple Systems	562
Related Procedure	564
Related Topics	564
Suspending or Resuming System Monitoring for a Single System	564
Related Procedure	565
Related Topics	565
Suspending or Resuming System Monitoring for Multiple Systems	565
Related Procedure	566
Related Topics	566
Version Control Repository	566
Related Topics	567
PMP Administrative Options	567
Related Topics	568
Setting Up Managed Systems	568
Overview	568
Installing Required and Optional managed system software	569
Installing the ProLiant Support Pack on Windows systems for the first time	569
Installing the ProLiant or Integrity Support Pack on a Linux system for the first time	576
Installing the required software on an HP-UX system	576
Configuring the Managed System Software	578

Run the Configure or Repair Agents feature from the CMS	578
Setting Up Managed Systems Manually	581
Setting Up HP-UX Managed Systems Manually	582
Setting Up Linux Managed Systems Manually	585
Examples	587
Setting up Windows managed systems	587
Setting up remote Linux systems from a Linux CMS	587
Setting up remote HP-UX systems from an HP-UX CMS	588
Related Topics	588
Managing SSH Keys	588
Related Procedures	589
Configuring SSH Key Security	589
Related Procedures	589
Related Topic	589
Importing an SSH Key	590
Related Procedures	590
Related Topic	590
Exporting an SSH Key	590
Related Procedures	591
Related Topic	591
Deleting an SSH Key	591
Related Procedures	591
Related Topic	591
Backing Up and Restoring the Database	591
Related Procedures	591
Related Topics	592
HP-UX/Linux	592
Backing up or Restoring the Database on the HP-UX or Linux Operating System	592
Related Procedure	592
Related Topic	592
Windows	592
Backing Up an SQL Server Database	593
Restoring the SQL Server Database from a Backup	593
Backing Up an MSDE Database	594
Backing Up HP SIM Using MSDE Command Line Features	594
Related Procedure	596
Related Topic	596
Configuring SSH Bypass Properties	596
Audit Log	597
Configuring the HP SIM Audit Log	597
Configuring the Tool Definition Files	597
Configuring the log.properties File	597
Related Topic	597
Viewing the Audit Log	597
Log Content	598
Related Topic	599
Configuring the Audit Log File	599
Related Topics	600
Troubleshooting	601
Authentication	601
Automatic Event Handling	601
Browser	601
CLI	605

CIMOM	606
Cluster	607
Collection	609
Custom Command	610
Database	610
Discovery	610
Event/SNMP Trap	611
Firmware Upgrade	612
Generic	612
HP SIM	613
HTTP Event	614
Identification	614
Integrated Lights-Out (iLO)	615
Internet Explorer	615
Installation	616
IP Address	618
OpenSSH	618
Operating System	618
Paging Notification	618
Ping	619
Printing	619
Property Pages	619
Protocol	620
Replicate Agent Settings	620
Response	621
Search	622
Security	622
Serviceguard Manager	622
Sign In	624
SNMP Agent	632
Software Status	632
Storage System	633
Switch	634
System	634
System Page	636
Task	637
Tools	638
VCRM	642
Virtual Machine	642
VMM	642
Windows NT Event Log	642
WMIMapper	643
Reference Information	644
Predefined Views	644
Database Tables	645
AuthenticationMethods_values table	646
CIM_ActiveConnection table	647
CIM_Chassis table	647
CIM_ComponentCS table	649
CIM_ComputerSystemPackage table	649
CIM_ComputerSystem table	649
CIM_ControlledBy table	650
CIM_DeviceSAPImplementation table	650
CIM_DeviceSoftwareIdentity table	650

CIM_ElementCapabilities table	651
CIM_HostedStoragePool table	651
CIM_IPProtocolEndpoint table	651
CIM_IPRoute table	651
CIM_iSCSICapabilities table	652
CIM_iSCSIConn_TCPProtoEnd table	653
CIM_iSCSIConnection table	653
CIM_iSCSISession table	653
SCSIProtoEnd_iSCSISession table	653
SCSIProtoEnd_NetworkPort table	654
CIM_LogicalDevice table	654
CIM_LogicalDisk table	655
CIM_LogicalPortGroup table	656
CIM_MediaAccessDevice table	656
CIM_NetworkAdapter table	658
CIM_MemberOfCollection table	661
CIM_NetworkPipeComposition table	661
CIM_NetworkPort table	661
CIM_OperatingSystem table	662
CIM_PhysicalElement table	664
CIM_PhysicalMedia table	666
CIM_PhysicalMemory table	669
CIM_PhysicalPackage table	670
CIM_PortController table	670
CIM_PowerSupply table	671
CIM_Process table	673
CIM_Processor table	675
CIM_Product table	678
CIM_RemoteServiceAccessPoint table	679
CIM_SCSIProtocolController table	679
CIM_SCSIProtocolEndpoint table	680
CIM_ProtoControlAccessesUnit table	680
CIM_ProtocolControllerForPort table	680
CIM_ProtocolControllerForUnit table	680
CIM_ProtocolEndpoint table	681
CIM_Rack table	681
CIM_Realizes table	681
CIM_Sensor table	682
CIM_SoftwareElement table	683
CIM_SoftwareIdentity table	685
CIM_StoragePool table	688
CIM_StorageVolume table	688
CIM_TCPProtocolEndpoint table	689
Classifications_values table	689
ComputerSys_HAP table	689
ComputerSys_LogicalPortGroup table	689
ComputerSys_NetworkPort table	690
ComputerSys_PortController table	690
ComputerSys_SAP table	690
ComputerSys_SCSIProtoCont table	690
ComputerSys_SCSIProtoEndp table	690
ComputerSys_SoftwareIdent table	690
ComputerSys_StorageVol table	691
DB_DeviceInfo table	691

DB_DeviceInfoEx table	691
DC_Enclosure table	692
DC_ProliantHost table	693
Dedicated_values table	694
DeviceNames table	694
Device Extended Attributes database table	695
Devices table	695
DeviceProtocolInfo table	697
ExtentStatus_values table	698
DeviceSnmpSettings table	698
HP_Cluster table	699
HP_Node table	699
HP_NParCabinet table	700
HP_NParCell table	700
HP_NParComplex table	702
HP_NParIOChassis table	703
HP_NParIOChassisSlot table	703
HP_NPartition table	703
HPUX_BaseKernelParameter table	704
HPUX_Bundle table	705
HPUX_DNSService table	708
HPUX_Fileset table	708
HPUX_HFS table	712
HPUX_LogicalVolume table	713
HPUX_NISServerService table	714
HPUX_NTPTService table	715
HPUX_PhysicalVolume table	716
HPUX_Product table	717
HPUX_VolumeGroup table	720
IPAddress table	721
IPProtocolEnd_NetworkPort table	721
IPXAddress table	722
OperationalStatus_SVvalues table	722
PhysicalPackage_Product table	722
SCSIProtoCont_SCSIProtoEnd table	722
SCSIProtocolCont_SoftwareId table	722
SCSIProtoEnd_SCSIProtoEnd table	723
NetworkAddresses_values table	723
NodeSnapshot table	723
NodeTypesEnum table	723
NodeSubTypesEnum table	724
Notices table	724
NoticeType table	725
OperationalStatus_CSvalues table	725
OperationalStatus_NPvalues table	726
operationalStatus_PCvalues table	726
Snapshot table	726
SPAllocatedFromStoragePool table	726
SVAllocatedFromStoragePool table	726
TCPProtoEnd_IPProtoEnd table	727
Windows Event Log	727
Windows NT/2000 Events	727
Windows NT/2000 Event Log Error Messages	727
Service and Support	728

Service and Support	728
glossary	730
Index	748

Legal Notices

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Warranty

A copy of the specific warranty terms applicable to your HP product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

Use of this documentation and any supporting software media supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and backup purposes only. Resale of the programs, in their present form or with alterations, is expressly prohibited.

Copyright Notice

© Copyright 2003-2005 Hewlett-Packard Development Company, L.P.

Trademark Notices

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32- and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95-branded products.

Intel, Celeron, Itanium, Pentium, and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java is a U.S. trademark of Sun Microsystems, Inc.

Linux is a U.S. registered trademark of Linus Torvalds.

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group.

Release History

Edition 4.0, November 2005

To ensure that you receive newer editions when they become available, subscribe to the appropriate product support service. See your HP sales representative for details.

Introduction

Online Help

HP Systems Insight Manager (HP SIM) provides an online help system to help you become familiar with its management features. It provides general information about using and administering HP SIM.

- **Opening the Help.** Click the **Help** icon on any page. The **Help** page opens in a separate window that you can move or resize. Most topics have links to **Related Procedures** and **Related Topics**.
- **Browsing for More Information.** You have the option of selecting topics from a table of contents, an index, and a search feature. Click the **Help** icon in the top menu frame to display the desired help topic you want to view. To open another topic, select the topic from the table of contents on the left side of the frame.

HP SIM Help Categories

The HP SIM help system covers the following categories:

- **Product Overview.** Provides you with an overview of the new features in HP SIM. Refer to “Product Overview” for more information.
- **Getting Started.** Includes procedures to begin using and administering HP SIM. Refer to “Getting Started” for more information.
- **Discovery and Identification.** Includes procedures to create and manage Discovery tasks, including identification, managing hosts files, and managing discovery templates. Refer to “Discovery and Identification” for more information.
- **Users and Authorizations.** Includes procedures to create manage users, user groups, toolboxes, and authorizations . Refer to “Users and Authorizations” for more information.
- **Networking and Security.** Includes information on networking and security, including setting up trust relationships. Refer to “Networking and Security” for more information.
- **Monitoring Systems, Events, and Clusters.** Includes procedures to begin monitoring your systems and events. Refer to “Monitoring Systems, Clusters, and Events” for more information.
- **Storage Integration.** Includes procedures for discovering SNMP and SMI-S storage devices and viewing information about them. Refer to “Storage Integration Using SNMP” and “Storage Integration Using SMI-S” for more information.
- **Managing with Tasks.** Includes procedures on how to manage your systems and events by scheduling and executing tasks. Refer to “Managing with Tasks” for more information.
- **Tools that Extend Management.** Includes procedures on how to use HP SIM default tools. Refer to “Tools that Extend Management” for more information.
- **Partner Applications.** Includes list of all partner applications as well as overview information for each. Refer to “Partner Applications” for more information.

- **Reporting.** Includes procedures on creating and generating custom reports. Refer to “Reporting” for more information.
- **Administering Systems and Events.** Includes information about managing and maintaining HP SIM. Information in this section pertains only to users with full-configuration-rights. Refer to “Administering Systems and Events” for more information.
- **Troubleshooting.** Includes information and tips to troubleshoot HP SIM. Refer to “Troubleshooting” for more information.
- **Reference.** Includes information on database tables, Windows NT error log messages, MSA tools, and service and support. Refer to “Reference Information” for more information.

Product Overview

HP Systems Insight Manager (HP SIM) combines the strengths of Insight Manager 7, HP Tootools, and HP Servicecontrol Manager to deliver a single tool for managing HP ProLiant, Integrity, and HP 9000 systems running Microsoft® Windows®, Linux, and HP-UX. The core HP SIM software delivers the essential capabilities required to manage all HP server platforms.

HP SIM can be extended to provide system management with plug-ins for HP clients, storage, power, and printer products. Plug-in applications for rapid deployment, performance management, partition management, and workload management enable you to pick the value-added software required to deliver complete lifecycle management for your hardware assets.

Additional Resources

For additional resources, go to the HP SIM website at <http://www.hp.com/go/hpsim>.

Related Topics

- Features
- What's New?
- Product Architecture
- Assistance
- Legal Notices

Features

HP Systems Insight Manager (HP SIM) provides the following features:

- **Easy and rapid installation.** Installs on your server platform of choice running HP-UX, Windows, or Linux, or on a Windows desktop or workstation.
- **First Time Wizard.** Provides you with step-by-step, online guidance for performing the initial configuration of HP SIM. The wizard helps you configure HP SIM settings on the central management server (CMS).
- **Automatic discovery and identification.** Automatically discovers and identifies systems attached to the network. Use discovery filters to prevent discovery of unwanted system types. Discovery filters enable you to limit discovery to specific network segments or IP address ranges.
- **Fault management and event handling.** Provides proactive notification of actual or impending component failure alerts. Automatic Event Handling enables you to configure actions to notify appropriate users of failures through e-mail, pager, or Short Message Service (SMS) gateway, and enables automatic execution of scripts or event forwarding to enterprise platforms, such as HP OpenView Network Node Manager or HP OpenView Operations.

Note:



Pager support is only for Windows-based CMS.

- **Consistent multi-system management.** Initiates a task on multiple systems or nodes from a single command on the CMS. This functionality eliminates the need for tedious, one-at-a-time operations on each system.
- **Secure remote management.** Leverages operating system security for user authentication and Secure Sockets Layer (SSL) and Secure Shell (SSH) to encrypt management communications.
- **Role-based security.** Enables effective delegation of management responsibilities by giving system administrators granular control over which users can perform which management operations on which systems.
- **Tool definitions.** Defines tools using simple XML documents that enable you to integrate off-the-shelf or custom tools. These tools can be command line tools, Web-based applications, or scripts. Access to these integrated tools is governed by role-based security.
- **Data collection and inventory reports.** Performs comprehensive system data collection and enables you to quickly produce detailed inventory reports for managed systems. Reports can be generated in HTML, XML, or CSV format.
- **Snapshot comparisons.** Enables you to compare configuration snapshots of up to four different servers or configuration snapshots of a single server over time. This functionally assists IT staff in pinpointing configuration issues that can contribute to system instability. Snapshot comparisons can also be used to save a picture of standard configuration for comparisons to other systems.
- **HP Version Control.** Automatically downloads the latest BIOS, driver, and agent updates for HP ProLiant servers running Windows and Linux, identifies systems running out-of-date system software, and enables system software updates across groups of servers. For HP-UX systems, Software Distributor is integrated into HP SIM.
- **Two user interfaces.** Provides a Web browser graphical user interface (GUI) and command line interface (CLI) to help incorporate HP SIM into your existing management processes.
- **Edit system properties on managed systems.** The **Edit System Properties** link on the **System Page** enables users with full-configuration-rights to re-configure system properties for a single system. To set system properties for multiple systems, select **Options->System Properties->Set System Properties**. This affects the system properties as reported by HP SIM, but does not change the properties on the target systems.
- **Suspend and resume monitoring of systems.** Enables you to set the timer for suspending monitoring. This enables a system to be excluded from status polling, identification, data collection, and the automatic event handling features of HP SIM. The **Suspend/Resume Monitoring** link under the **Tools & Links** tab of the **System Page** enables you to set the timer for suspending or resuming system monitoring. To suspend or resume system monitoring for multiple systems, select **Options->System Properties->Suspend or Resume Monitoring**.

The available suspend lengths include the predetermined increments of five minutes, 15 minutes, one hour and one day. The suspend feature can be turned on indefinitely.

- **Install OpenSSH tool.** Runs from the CMS and installs the OpenSSH service onto target Windows systems and then runs the `mxagentconfig` command to complete the configuration.

Note:



This is only available on Windows CMS.

- **Initial ProLiant Support Pack Install optionally installs OpenSSH.** HP SIM enables you to install OpenSSH through the Initial ProLiant Support Pack Install process by selecting **Install and initialize OpenSSH (Secure Shell)** on the **Initial ProLiant Support Pack Install** page.

Note:



This is only available on Windows CMS.

- **Support for HP-UX Serviceguard clusters.** HP SIM recognizes HP-UX Serviceguard clusters and displays them in the UI. HP Serviceguard Manager is opened by clicking a Serviceguard cluster in a search list, and provides information on the clusters.
- **WBEM Indications for HP-UX, Linux, and SMI-S devices.** HP SIM enables you to subscribe and unsubscribe to WBEM indications through the GUI. You can also subscribe or unsubscribe to WBEM indications from the CLI. For HP-UX, this feature is only available on 11i v2 September 2004.
- **HP Instant Support Enterprise Edition (ISEE).** HP Instant Support Enterprise Edition (ISEE) is a proactive remote monitoring and diagnostic tool to help manage your systems and devices, a feature of HP support. ISEE gives you simple, unified approach to monitoring your entire datacenter. Instead of using separate technologies for each of your platforms, you can monitor and manage a diverse IT environment with a single solution. ISEE helps you proactively manage and support HP-UX, Microsoft Windows, Linux, OpenVMS, Tru64 UNIX, NonStop and Sun Solaris servers, connected peripherals, and storage and network devices. It reduces cost and complexity by supporting both mission critical and non-mission critical systems and devices. ISEE provides continuous hardware event monitoring and automated notification to identify and prevent potential critical problems. Through remote diagnostic scripts and vital system configuration information collected about your systems, ISEE enables fast restoration of your systems. Install ISEE on your systems to help mitigate risk and prevent potential critical problems.
- **HP System Management Homepage.** The System Management Homepage is a Web-based application that provides a consolidated interface for single system management. By aggregating the data from HP Web-based agents and management utilities, the System

Management Homepage provides a common, easy-to-use interface for displaying hardware fault and status monitoring, performance data, system thresholds, diagnostics, and software version control for an individual server.

- **Performance Management Pack (PMP) access.** A software solution that detects, analyzes, and explains hardware bottlenecks on HP ProLiant servers and Modular Shared Array (MSA) shared storage. PMP tools available in HP SIM consist of Online Analysis, Offline Analysis, CSV File Generator Report, System Summary Report, Static Analysis Report, Configuration, Licensing, and Manual Log Purge. PMP is automatically installed with HP SIM and operates in integration with HP SIM. No software installation on the monitored servers is required, other than the Insight Management Agents. PMP 4.0 includes:

- Support for HP SIM 5.0 (this version of PMP does not support HP SIM 4.x)
- Support for Oracle database (locally or remote)
- Support for select HP Integrity servers

New in PMP v4.0.1:

- Support for Red Hat Linux 4.0
- Support for HP ProLiant BL25p servers
- Provides an option to remove or retain old PMP database files during the installation process

Refer to

<http://h18013.www1.hp.com/products/servers/proliantessentials/valuepack/pmp/index.html> for more information.

- **HP ProLiant Essentials Vulnerability and Patch Management Pack (VPM) access.** VPM identifies and provides advice to resolve security vulnerabilities and delivers advanced patch management through automated acquisition, optimized deployment, and continuous enforcement of security patches. VPM must be manually installed from the Management CD and requires one license for each target system being managed. Five fully functional non-expiring licenses, for use on servers or desktops, are provided with VPM for evaluation purposes. For more information about installation and setup, refer to the *HP ProLiant Essentials Vulnerability and Patch Management Pack Quick Setup Poster* and the *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide*, both on the Management CD. For more information on VPM, go to HP ProLiant Essentials Vulnerability and Patch Management Pack at <http://www.hp.com/servers/proliantessentials/vpm>.

- **HP ProLiant Essentials Virtualization Management Software (VS).** Virtual machine management capabilities integrated into HP SIM extends its capabilities to deliver unified management of an IT infrastructure consisting of both physical and virtual server resources, simplifying and consolidating the provisioning, management and migration of all server resources from one central interface.

The virtual machine management capabilities in HP SIM are provided by integrating the HP ProLiant Essentials Virtual Machine Management Pack (VMM) and the HP ProLiant Essentials Server Migration Pack (SMP). Both these components are installed together as one component, but licensed separately.

- **HP ProLiant Essentials Virtual Machine Management Pack.** VMM provides central management and control for virtual machines of type Microsoft's Virtual Server and VMware's GSX or ESX. Using VMM, all virtual machines and Virtual Machine (VM) hosts

can be managed from the HP Systems Insight Manager (HP SIM) console. The **Virtual Machine Management Pack** displays a tree view of the VM hosts and VM guests in the left pane of the HP SIM console. After selecting a system in the left pane tree, information for the system selected is displayed in the right pane. You then have options to deploy, register, unregister, and upgrade. VMM is now integrated into HP SIM, Refer to <http://www.hp.com/servers/proliantessentials/vmm> for documentation and more information on VMM.

- **HP ProLiant Essentials Server Migration Pack.** SMP extends the functionality of the VMM to provide integrated Physical-to-Virtual (P2V) and Virtual-to-Virtual (V2V) migrations. The SMP enables you to simplify the server consolidation process, thereby freeing you to focus on other priorities. SMP now offers a new SMP license type that allows unlimited migrations for one year after the first migration is initiated. To purchase additional licenses, refer to <http://www.hp.com/servers/proliantessentials/smp>.

- **HP BladeSystem Integrated Manager in HP Systems Insight Manager.** HP SIM delivers a blade environment designed to consolidate access to blade deployment, configuration, and monitoring tools. Picture views are available of racks and enclosures. HP BladeSystem Integrated Manager is automatically installed with HP SIM, no license key is required. To access HP BladeSystem Integrated Manager, select **Tools->Integrated Consoles->HP BladeSystem**. Refer to <http://h18004.www1.hp.com/products/servers/management/bsme/index.html> for more information.

- **HP Configure or Repair Agents.** The Configure or Repair Agents feature is an HP SIM feature that enables you to repair credentials for SNMP settings, System Management Homepage or Management HTTP Server trust relationships on Windows, Linux, and HP-UX systems supported by HP SIM. For more information, refer to the Configure or Repair Agents Online Help at <http://h18000.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **HP ProLiant Essentials Rapid Deployment Pack (RDP) - Windows Edition.** RDP is a multiserver deployment tool that enables IT administrators to easily deploy large volumes of servers in an unattended, automated fashion. RDP is installed separately from HP SIM and requires a license for each server being managed. RDP is installed from its own CD. Refer to <http://www.hp.com/servers/rdp> for information about network environment setup, prerequisites for the deployment server, and installation instructions. When installed, you must register your product registration number to receive a license file. A license is required for each server being managed by RDP.

- **Data collection and inventory reports for Superdomes and other complexes.** Data collection and reporting has been added for Superdome systems and other cellular complexes. The type of data that can be collected includes information on chassis, cabinets, cells, memory, and hard partitions (nPars). The type of data actually collected depends on which filters are selected.

- **HP Storage Essentials.** HP is changing the economics of management in the data center. HP Storage Essentials is the first open, standards-based suite of storage products designed to integrate into HP's unified server-storage management platform, HP SIM. For more information on HP Storage Essentials, go to <http://h18006.www1.hp.com/products/storage/software/esuite/index.html>.

- **Manage SSH Keys.** The **SSH Keys** feature enables you to view and manage the public SSH keys, stored in the `known_hosts` file, from the central management server. SSH keys

enable the central management server and a managed system to authenticate a secure connection.

Related Topics

- What's New?
- Product Architecture
- Assistance
- Legal Notices
- Getting Started

What's New?

HP Systems Insight Manager (HP SIM) has a very robust functionality set that is cross-platform compatible. To make the product easier to use, the menu items across the top of the product (**Tools**, **Deploy**, and so on) are dynamic depending on what systems you have discovered in your environment. For example, if you have not discovered any HP-UX systems, then you will not see any HP-UX specific commands like **Optimize->Process Resource Manager**.

What's New for HP SIM 5.0?

- New look for the graphical user interface (GUI) which has the look and feel of other HP products.
- HP SIM no longer requires JRE to be installed on the client systems.
- Discover storage systems through their installed SMI-S providers. Refer to <http://www.hp.com/go/hpsim/providers> for information about the supported devices and SMI-S providers.
- Cluster Monitor monitors MSCS clusters only.
- Reports are now available in XML format.
- New report engine along with new default reports.
Refer to "Reporting Views" for more information.
- View a consolidated list of all server and storage events from a single event viewer, and configure and take automated actions.
- View storage array capacity details, including unallocated space, RAID overhead, usable bytes assigned to ports, and usable bytes not assigned to ports.
- Flexible role-based security enables you to decide which administrators have access to server and storage details.
- Enables you to launch server and storage element managers from a single system viewer.
- Lists and folders are now called collections.
- Ability to assign privileges to operating system user groups to give these users access to HP SIM without creating each individual user.

Refer to "Creating New User Groups" for more information.

- Improved access to discovery options which includes a **Discovery** page with tabs for **Automatic**, **Manual**, and **Hosts Files** configuration.

Refer to “Discovery and Identification” for more information.

- New command line interface (CLI) commands, including mxreport, mxcert, mxglobalprotocolsettings, mxglobalsettings, mxcollections, and mxgethostname.

Refer to “Using Command Line Interface Commands” for more information.

- Ability to set system properties for multiple systems at the same time.

Refer to “Editing System Properties for Multiple Systems” for more information.

- Ability to suspend or resume monitoring of multiple systems at the same time.

Refer to “Suspending or Resuming System Monitoring for Multiple Systems” for more information.

- New tree view available for system and cluster collections.

Refer to “Navigating the Tree View” for more information.

- Ability to create, edit, and delete discovery tasks.

Refer to “Discovery and Identification” for more information.

- Ability to create new command line tools including copying a file, removing a tool, and creating command line, Web launch, and X window tools on HP-UX and Linux systems.

Refer to “Command Line Tools” for more information.

- Supports the use of an Oracle database (locally or remotely) for Windows, HP-UX, and Linux.

Refer to the HP Systems Insight Manager Installation and User Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for additional information.

- Added support for managed system configuration to include Linux, HP-UX, and Windows operating systems.

Refer to Configure or Repair Agents Online Help at <http://h18000.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information.

- First Time Wizard that provides you with step-by-step, online guidance for performing the initial configuration of HP SIM, and helps you configure HP SIM settings on the central management server (CMS)

Refer to “First Time Wizard” for more information

- The HP Services analysis tools, Web-Based Enterprise Services (WEBES), and Open Service Event Manager (OSEM), generate service notifications to HP SIM through a specific SNMP trap type if analysis has determined there are serviceable events. If Instant Support Enterprise Edition (ISEE) is installed, the service notification provided by WEBES and OSEM also provide status about the remote support incident.

Related Topics

- Features
- Product Architecture
- Assistance
- Legal Notices
- Getting Started

Product Architecture

HP Systems Insight Manager (HP SIM) leverages a distributed architecture that can be broken into three types of systems (central management server (CMS), managed systems, and network clients).

The CMS and the managed systems together are called the HP SIM management domain.

Central Management Server

Each management domain has a single CMS. The CMS is the system in the management domain that executes the HP SIM software and initiates all central operations within the domain. In addition to the HP SIM software, the CMS maintains a database for storage of persistent objects and it can reside on a separate system. Typically, applications for the multiple-system aware (MSA) tools also reside on the CMS. These applications are not required to reside on the CMS. They can reside anywhere on the network.

Because the CMS is a system within the management environment, it manages itself as part of the domain. You can add the CMS as a managed system within another management domain if you want to manage it using a separate CMS.

Managed Systems

Systems that make up a management domain are called managed systems. A system can be any device on the network that can communicate with HP SIM, which includes servers, desktops, laptops, printers, workstations, hubs, storage systems, SANs, and routers. In most cases, these devices have an IP address or IPX address associated with them. A managed system can be managed by more than one CMS if desired.

Systems to be managed must have one or more management agents installed. There are a wide variety of agents, such as the ProLiant management agents based on SNMP, WMI found on Windows systems, or WBEM providers, such as the System Fault Management providers for HP-UX. Those agents provide management information and alerts (indications) to the CMS. The SSH agent (service) then enables the HP SIM CMS to log into the managed system to execute commands through scripts.

Note:



IPX systems can only be discovered and managed on a Windows CMS.

System Collections

System collections provide a way to group systems in the HP SIM database. A collection can be used to filter systems that share common attributes, such as operating system type or hardware type. System collections can also be arbitrary collections of systems. Systems can belong to one or more system collections. Many default shared system collections are provided, and users can create their own shared and private collections. Working with system collections increases your efficiency because you can perform a task on each system in a system collection with a single step. Refer to “Shared System Collections” for a complete list of all shared system collections.

Network Clients

HP SIM can be accessed from any network client. The network client can be part of the management domain. The network clients must be running a compatible browser to access the graphical user interface (GUI) or a Secure Shell (SSH) client application to securely access the command line interface (CLI).

Note:



Access to the Web server on the CMS can be restricted to specific IP address ranges for specific users.

Related Topics

- Features
- What's New?
- Assistance
- Legal Notices
- Getting Started

Assistance

Additional Resources

For additional resources, go to the:

- HP Systems Insight Manager (HP SIM) website at <http://www.hp.com/go/hpsim/> for general product information and links to software downloads, documentation, and troubleshooting information
- HP Technical Documentation website at <http://www.docs.hp.com/> for access to HP SIM manuals and release notes
- HP Software Depot website at <http://www.software.hp.com/> for access to HP SIM software downloads
- HP Business Support Center website at <http://www.hp.com/bizsupport/> for support information about HP SIM and HP Commercial products

- HP IT Resource Center website at <http://www.itrc.hp.com> for support information about HP SIM and HP Enterprise products
- HP SIM SMI-S Providers web page at <http://www.hp.com/go/hpsim/providers> for information about device support and SMI-S providers.

Technical Support

Technical support is available during normal business hours through the HP World-Wide Response Centers for customers with appropriate support agreements.

Related Topics

- Resource Library
- Features
- What's New?
- Product Architecture
- Legal Notices
- Getting Started

Getting Started

If you are just getting started with HP Systems Insight Manager (HP SIM), you must familiarize yourself with the software and set it up for your environment. First, familiarize yourself with the product by reviewing the information in the “Product Overview” section. Then, complete the recommended steps for getting started with that permission level.

- Sign into the graphical user interface (GUI). Refer to “Signing In” for details.
- Familiarize yourself with the HP SIM **Home** page. Refer to “Navigating the Home Page” for details.
- Perform the initial setup if this is a new installation. Otherwise, review the steps involved with initial set up to familiarize yourself with the basic management tasks. Refer to “Performing Initial Setup” for details. This is available to users with full-configuration-rights only.
- Familiarize yourself with how to schedule and execute tasks. Refer to “Managing with Tasks” for details.
- Familiarize yourself with the HP SIM reporting features. Refer to “Reporting” for details.
- Review the HP SIM commands if you intend to use the command line interface (CLI). Refer to “Using Command Line Interface Commands” for details. This is available to users with full-configuration-rights only.
- Customize the **Home** page and the **System Status** panel. Refer to “Customizing the Home Page” and “Customizing the System Status Panel” for details.

Related Procedures

- Signing In
- Signing Out
- Navigating the Home Page
- Performing Initial Setup
- Using Command Line Interface Commands
- Customizing the Home Page
- Customizing the System Status Panel

Related Topics

- Product Overview
- Monitoring Systems, Clusters, and Events
- Managing with Tasks
- Administering Systems and Events

Signing In

Access the graphical user interface (GUI) using a Web browser or the command line interface (CLI) using a Secure Shell (SSH) client.

When you first sign into HP Systems Insight Manager (HP SIM) the **First Time Wizard** popup window appears. The First Time Wizard provides information and procedures for getting started with HP SIM. Click **Close** to exit the window. If you do not want this window to display each time you sign into HP SIM, select **Do not automatically show this wizard again** and then click **Close**. Refer to “First Time Wizard” for more information.

Signing into the GUI

Access the HP SIM GUI from any network client using a Web browser. For information about which browsers are supported, refer to the HP Systems Insight Manager Installation and User Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

Note:



After accessing HP SIM, if you open additional windows in the same browser process and navigate to the same HP SIM URL you navigated to previously, you do not need to sign back into HP SIM. Any time you start a new instance of the browser process and navigate to HP SIM, you must sign in.

If you sign into HP SIM and then navigate to a different site entirely, the HP SIM session begins to time out. If you use the same browser process to return to HP SIM in under 20 minutes, you are not required to sign back in. Otherwise, you must sign in again.

Note:



If you browse to the central management server (CMS) from a Windows 2003 system and you have problems browsing, you may need to configure your browser to trust the CMS. To do this:

1. On the system browsing to the CMS, select **Start->Settings->Control Panel->Internet Options->Security->Trusted Sites**, and then click **Sites**.
2. In the **Add this Web site to the zone**, enter the CMS, or click **Add**. Add the system as **https://<cms name>:50000**.
3. Click **OK** to add the CMS.

To sign into the GUI:

1. Open a supported Web browser on any network client, and enter the address for the sign in page by navigating to **http://hostname:280/**, where *hostname* is the hostname of the CMS.

Note: If you are signing in directly on a Windows CMS, you can use the **HP SIM** desktop icon to access the sign in page, or you can select **Start->Programs->HP Systems Insight Manager->HP Systems Insight Manager**.

2. Enter your **User name**, **Password**, **Domain**, and **Time zone** if requested.

Note: If the browser can determine its time zone with certainty, then the **Time zone** selection field is not displayed.

3. Click **Sign In**.

Signing In Using SSL

If your browser is not configured with the Secure Sockets Layer (SSL) system certificate of the HP SIM system, a Security Alert regarding a certificate of untrusted origin might appear when first browsing to HP SIM using SSL. If a Security Alert appears, perform one of the following procedures:

- Import the certificate into your browser now, using the browser. View the certificate by double-clicking the lock icon, and then install it. Refer to “Importing a Server Certificate” for more information.
- Export the HP SIM System Certificate to a file by first browsing from a local browser on the HP SIM system. Then, manually import it into the remote browser. Refer to “Exporting a Server Certificate” for more information.
- Sign into the HP SIM system this time without a trusted certificate, but resolve to import the certificate in the future. Your data is still encrypted.

Caution:



If you cannot ensure that the HP SIM system to which you are browsing is, in fact, the HP SIM system you believe it is, do not select of the last two SSL options. You could be giving your sign in credentials to a rogue system disguised as your HP SIM system, or you could be importing a certificate from a rogue system disguised as your HP SIM system and subsequently giving your sign in credentials to that rogue system.

After you have an SSL session established with HP SIM, all communications between the browser and HP SIM are secure through SSL.

Logging into the CLI

Access the HP SIM CLI directly on the CMS or from any network client using SSH client software.

Note:



On a Windows CMS, some commands require that the user be a member of the local Administrators group. This list of commands includes:

- mxagentconfig
- mxauth
- mxcert
- mxcollection
- mxexec

- mxgetdbinfo
- mxglobalprotocolsettings
- mxglobalsettings
- mxlog
- mxmib
- mxngroup
- mxnode
- mxnodesecurity
- mxoracleconfig
- mxpassword
- mxquery
- mxreport
- mxstm
- mxtask
- mxtool
- mxtoolbox
- mxuser
- mxwbemsub

Logging in Directly on the CMS

1. Log into the CMS using a valid user name and password (SSH `system name`).
HP SIM grants authorizations based on your OS user login.
2. Open a terminal window or a command prompt window to execute HP SIM commands.

Remotely Using an SSH Client

Note:



The preferred way to log in remotely is using an SSH client. Telnet or rlogin work, but neither provides a secure connection.

1. Open an SSH client application on any network client.
2. Log into the CMS through the SSH client software, using a valid user name and password.

HP SIM grants authorizations based on your OS user login.

Related Topics

- Getting Started
- Signing Out
- Using Command Line Interface Commands
- Networking and Security

Signing Out

Sign out from HP Systems Insight Manager (HP SIM) to prevent someone from accessing your active session if you walk away.

If you are monitoring HP SIM, your session remains alive and is continually refreshed unless you close the browser or navigate to another site. In this case, HP SIM signs you out after 20 minutes. As long as you are actively working in HP SIM, the session stays alive. However, HP SIM ends your session and signs you out after 20 minutes of inactivity. Refer to the HP Systems Insight Manager Installation and User Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> in Chapter 14 in the *GUI Time-Out Policy* section more information on keeping sessions alive.

Signing Out from the Graphical User Interface (GUI)

To sign out from the GUI:

1. Click **Sign Out** in the HP SIM banner.
2. Close the Web browser.

Signing Out from the Command Line Interface (CLI)

To sign out from the CLI, log off of the CMS or the Secure Shell (SSH) client application.

Related Topics

- Getting Started
- Signing In

First Time Wizard

The First Time Wizard provides you with step-by-step, online guidance for performing the initial configuration of HP Systems Insight Manager (HP SIM). The wizard helps you configure the following HP SIM settings on the central management server (CMS).

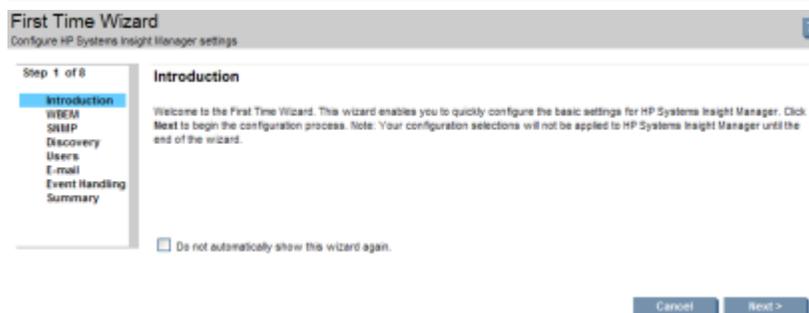
- WBEM protocol
- SNMP protocol

- Automatic Discovery
- User settings
- E-mail settings
- Automatic Event Handling

Note:



When **Automatic Discovery** is selected, discovery runs when you exit the First Time Wizard. When it is deselected, which is the default, you must enable the default **System Automatic Discovery** task for discovery to run. Select **Options->Discovery**, and select **System Automatic Discovery** task. Click **Enable**, to enable this task.



The wizard starts the first time a user with full-configuration-rights logs into HP SIM. If the wizard is canceled prior to completion, it restarts each time a user with full-configuration-rights signs in. You can cancel and disable the wizard from automatically starting by selecting the **Do not automatically show this wizard again** checkbox. The wizard can be manually started by selecting **Options->First Time Wizard**. The **First Time Wizard Introduction** page appears.

Review your selections on the **Summary Page** and click **Finish** to save the settings. Automatic discovery runs immediately to populate the HP SIM database.

Note:



The First Time Wizard configures only the basic settings in HP SIM. Refer to the **Related Procedures** and **Related Topics** for more detailed information.

Related Procedures

- Setting Global Protocols
- Configuring Discovery General Settings
- Configuring Automatic Discovery
- Creating a New Discovery Task
- Users and User Groups
- Creating New Users

- Deleting User Accounts and User Groups
- Configuring E-mail Settings
- Creating an Automatic Event Handling Task with Selected Event and System Attributes

Related Topics

- Administering Systems and Events
- Protocols
- WBEM Indications
- Data Collection
- Discovery and Identification
- Events
- About Administering Events

Performing Initial Setup

The initial setup involves setting up managed systems, configuring discovery, configuring event handling, adding users, and defining authorizations. It assumes that you just completed the installation of your central management server (CMS). If you skipped or canceled the First Time Wizard, the following steps assist you in setting up your environment to run HP Systems Insight Manager (HP SIM).

If you are new administrator of an existing management domain, it might be useful for you to familiarize yourself with these steps even though your CMS has already been through the initial setup. The steps in this process are common tasks that HP SIM administrators perform on a regular basis.

Initial Setup Process

When you first start HP SIM, the introductory page appears with a section called **DO THIS NOW to finish the install**. To get started using HP SIM:

1. **Set up managed systems.** Setting up managed systems involves installing the required management agents and configuring HP SIM software. Refer to “Setting Up Managed Systems” for more information.
2. **Configure protocol settings.** Configuring the protocol settings defines what systems are added to HP SIM using discovery in the next step. Refer to “Setting Global Protocols” for more information.

If you ran the First Time Wizard, the protocol settings might already be configured.

3. **Configure Discovery: Automatic or Manual.** Discovery is the process that HP SIM uses to find and identify the systems on your network and populate the database with that information. A system must first be discovered to collect data and track system health status. There are two ways to discover new systems:
 - **Automatic discovery.** Searches the network for systems running specific protocols. It runs automatically every 24 hours, but the process can be manually executed or scheduled to execute at other times.

If you ran the First Time Wizard, discovery might already be completed.

- **Manual discovery.** Used to add a single system or a group of systems using a Hosts file.

Refer to “Configuring Automatic Discovery” for information on Automatic Discovery or “Adding a System Manually” for information on Manual Discovery.

4. **Add new users.** Any user with a valid network login can be added to HP SIM. Refer to “Users and User Groups” for more information.

If you ran the First Time Wizard, new users might already be added.

5. **Configure e-mail settings.** Configuring e-mail settings enables users to receive e-mail notification of certain events. Refer to “Configuring E-mail Settings” for information on e-mail settings.
6. **Configure paging settings.** Configuring paging settings enables users to receive pages that notify them of certain events. Refer to “Configuring Modem Settings” for information on paging settings.
7. **Setup automatic event handling.** Automatic event handling enables you to define an action that HP SIM performs when an event is received. Automatic event handling can be set up to use the e-mail and paging settings that you specified in the previous sections. Refer to “Creating an Automatic Event Handling Task with Selected Event and System Attributes” and “Creating an Automatic Event Handling Task with an Existing Event Collection ” for more information.

Related Topics

- Signing In
- Signing Out
- Navigating the Home Page

Navigating the Home Page

Graphical User Interface Features

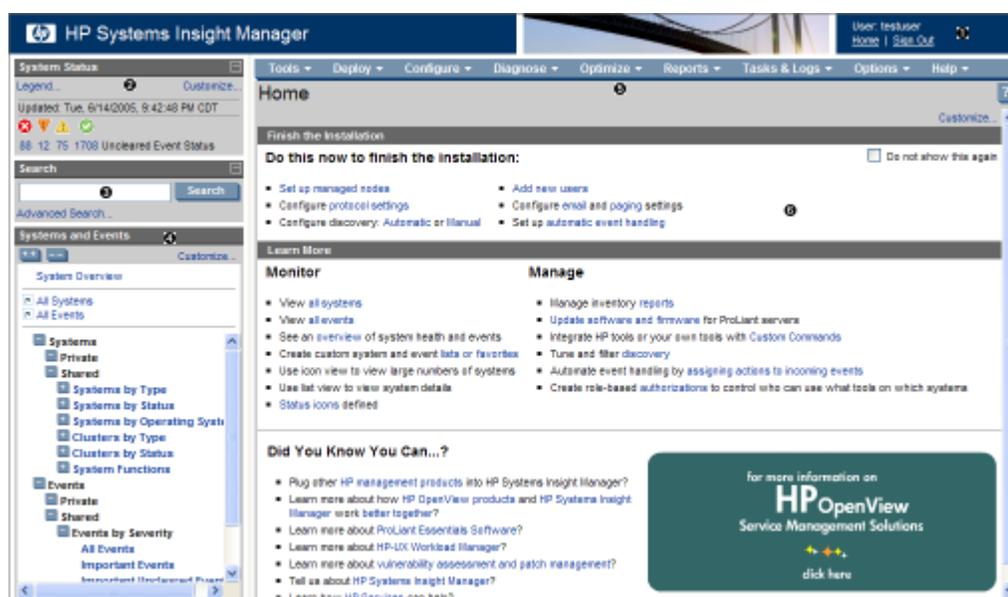
This section describes the graphical user interface (GUI) features. The following figure is a sample screen shot of the GUI.

The five regions in the GUI include:

1. **Banner.** The banner provides a link to the **Home** page, a link to **Sign Out** of HP Systems Insight Manager (HP SIM), and displays the user that is currently signed in.
2. **System Status Panel.** This panel provides uncleared event status, system health status information, and an alarm to notify you of certain events or statuses. The **System Status** panel can be customized for your environment. If you do not need to view this panel at all times, you can collapse it by clicking the minus sign in the top right corner of the panel. To expand the panel, click the plus sign again. If the **System Status** panel is collapsed and an alarm is received, the panel expands to show the alarm.
3. **Search Panel.** The search feature enables you to search for matches by system name and common system attributes. You can also perform an advanced search for matches based on selected criteria. If you do not need to view this panel at all times, you can collapse it by

clicking the minus sign in the top right corner of the panel. To expand the panel, click the plus sign again. Refer to “Basic and Advanced Search” for more information.

4. **System and Event Collections.** System and event collections enable you to view all known systems and events of a specific subset. Collections can be private, visible only to its creator, or shared, visible by all users. HP SIM ships with default shared collections only. Refer to “Monitoring Systems, Clusters, and Events” for information about customizing and creating new collections. Refer to “Default Public Collections” for more information on the default shared collections shipped with HP SIM.
5. **Menus.** The HP SIM menus provide access to tools, logs, software options, and online help. The **Options** menu is primarily targeted for users who administer the HP SIM software. If you lack authorization to use these tools, you might not be able to access this menu.
6. **Workspace.** The workspace displays the results of your latest request. It can contain a collection, tool, or report. Some tools launch a separate browser window or X Window terminal instead of displaying in the workspace. This area contains the **Home** page when you sign into HP SIM. By default, the introductory page appears as the **Home** page.



Default Home Page Features

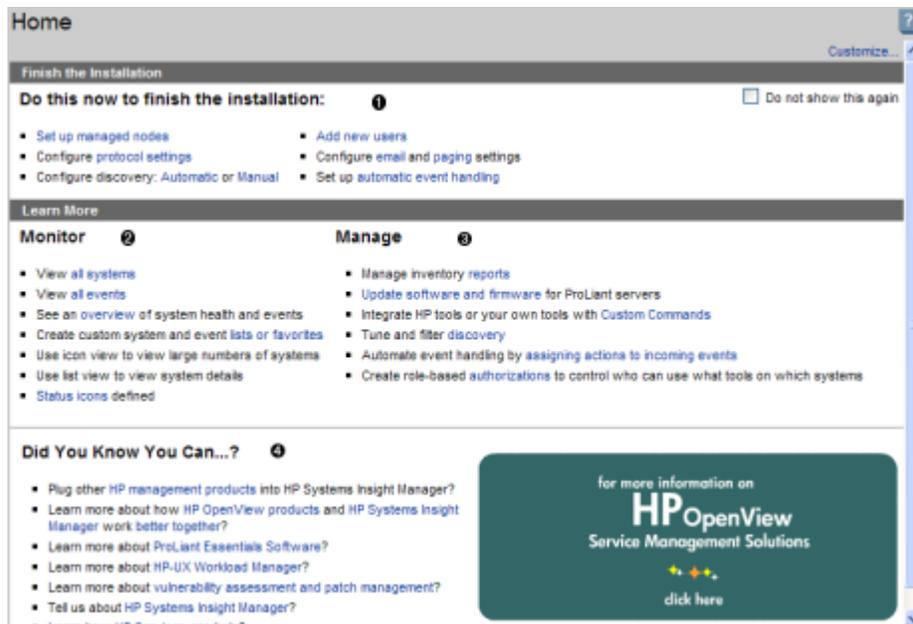
The HP SIM introductory page is the default **Home** page for the GUI. The introductory page provides information and tips about HP SIM and links to frequently used features. You can customize HP SIM to display a different page as the **Home** page. Refer to “Customizing the Home Page” for information on selecting a different introductory page. The following figure is a sample screen shot of the introductory page.

The four default sections on the introductory page include:

1. **Do this now to finish the installation:** This section only appears if the following conditions are met:
 - The user has full-configuration-rights.
 - The user has not disabled this section from the **Home Page Settings** page.

2. **Monitor.** This section provides links to common monitoring tasks, including locating and tracking systems and events. All monitoring tasks can be performed using the features and tools provided in the system and event collection area.
3. **Manage.** This section provides links to frequently used tools and features available from the menus above the workspace. These links provide access to inventory reports, software and firmware deployment, discovery, event handling, integrating custom commands, and authorizations.
4. **Did You Know You Can...?** This section provides useful tips and shortcuts, where you can learn more about HP products, service offerings, and software.

This section appears if you have not disabled it from the **Home Page Settings** page.



Related Topics

- Customizing the Home Page
- Customizing the System Status Panel

Customizing the Home Page

Customize the **Home** page to select which pages display and customize the regions on the default **Home** page and introductory page.

To customize the **Home** page:

1. Click **Home** in the banner to display the **Home** page in the workspace.
2. Click **Customize** in the upper right corner of the introductory page.

Note: If the **Home** page has been set to something other than the default introductory page, you can access the **Home Page Settings** page by selecting **Options->Home Page Settings**.

3. Specify which page you want to use as **Home** page:

- Introductory page (default)
- System Overview page
- Any specific system, cluster, or event collection

Note: The default introductory page is only available when it is set as the **Home** page. If you want to view this page when it is not set as your home page, reselect it as the **Home** page.

4. (Optional) If the introductory page is selected as your home page, customize the content on the page by selecting or deselecting:
 - **Show "Do this now to finish the install" frame.** If selected, this section appears on the **Home** page.
 - **Show the "Did You Know?" image.** If selected, the image in the bottom right corner of the **Home** page appears.

Related Topics

- Navigating the Home Page
- Customizing the System Status Panel

Customizing the System Status Panel

Customize the **System Status** panel to display the following status information:

- **Uncleared Event Status.** A count that indicates the number of uncleared event statuses that are Critical, Major, Minor, and Normal for any given system collection. Each number is a hyperlink to a detailed list of events with that particular status. By clicking the number, an event collection appears with those particular events and their corresponding systems.
- **Health Status.** A count that indicates the number of systems, in a given system collection, that have a system health status that is Critical, Major, Minor, and Normal. Each number is a hyperlink to a detailed list of systems with that particular status. By clicking the number, a system collection appears with those particular systems. Health status is not shown by default but can be configured to appear.
- **Alarm.** An alarm can be customized to appear for specific criteria for any given system collection. The alarm alerts you that a particular criterion has been met by one or more systems in that collection. Because the Status panel is continually updated, the alarm appears until the event is cleared, the system is removed from the collection, or the alarm customization is changed so that it no longer applies. If the **System Status** panel is collapsed, and an alarm occurs, it opens automatically so that the alarm is visible. You can collapse the panel, but it continues to open as long as the alarm is relevant. To have the panel remain collapsed, you must clear the offending event or system status or reconfigure the status display to no longer display alarms.
- **Legend of Status Icons.** To display a list of status icons, click **Legend** in the **System Status** panel. Legend information appears in a popup window and remains open until you close it. Refer to "System Status Types" for more information on default user templates.

Note:



If the **System Status** panel is customized to have no status displayed, the timestamp does not display.

To customize the **System Status** panel:

1. Click **Customize** in the upper right corner of the **System Status** panel. The **Customize System Status** page appears.
2. Select the first **Show summary of**, and select **uncleared event status** or **health status**.
 - a. Select the system collection **All Systems**, or select another system collection from the dropdown list.
 - b. Edit the **Label** if desired.
3. Select the second **Show summary of**, and select **uncleared event status** or **health status**.
 - a. Select the system collection **All Systems**, or select another system collection from the dropdown list.
 - b. Edit the **Label** if desired.
4. Select to **Show an alarm when any system meets the condition**.
 - a. Select the **Condition**.
 - b. Select the system collection **All Systems**, or select another system collection from the dropdown list.
 - c. Edit the **Label** if desired.
5. Click **OK** to save changes.

Note: Restore Defaults returns the customization screen to its default condition: only the uncleared event status appears in the banner. Health status and the alarm are disabled. All personalized information is removed.

Related Topics

- Navigating the Home Page
- Customizing the Home Page
- System Status Types

Setting Language Locale

Introduction

You can set the language or locale in your operating system, in a command shell, or in your Web browser to English or Japanese and run HP Systems Insight Manager (HP SIM). Both the central management server (CMS) and the managed systems must have support for all of the desired languages installed. The language is used to present all the labels, menus, and status and error messages in HP SIM in the requested language. The graphical user interface (GUI) shown in your browser appears in the preferred language of the Web browser. Also, tools and tasks executed interactively through the CMS have the same language used as the language the tool command line is executed with on the target system. This enables your Web browser to run tools, create scheduled tasks, and manually run scheduled tasks in the preferred language. Likewise, the language setting of your command shell is forwarded through the **mxexec** and **mxtask** command line commands to set the language for executing a tool, manually executing a task, or creating a scheduled task when the command line for the tool is executed on the target systems.

The CMS also has another locale independent from any user sessions (refer to “Configuring HP SIM”). This is referred to as the CMS Locale. Some of the features inherit this locale, such as logging files and e-mail messages sent by Automatic Event Handling which are neutral from any sessions.

Setting the Web Browser Language or Locale

When you configure your Web browser and select the language you prefer, the HP SIM GUI honors this request. This is for English and Japanese only. The browser locale is also used to set the language and encoding in the Secure Shell (SSH) command shell in which the tool command executes. The browser locale is saved on a scheduled task when it is created and is used to set the language and encoding on the target system for Single-system Aware (SSA) tools and on the execution system for Multiple-system Aware (MSA) tools. When you manually execute a task, the current browser locale overrides the locale set in the scheduled task for this single manual execution of the task (for SSA and MSA tools).

Configuring the Language Settings in Internet Explorer

Complete the following procedure to set the preferred language settings to Japanese in Internet Explorer.

1. Select **Tools->Internet Options->[Languages]**. The **Language Preference** window appears.
2. Click **Add**. The **Add Language** window appears.
3. Select **Japanese** from the list.
4. Click **OK** to add it to the language preference list.
5. Select **Japanese** in the language preference list and click **Move Up** until it is at the top of the list, or select and remove any other languages listed here.
6. Click **OK**. Continue to click **OK** until you have closed all windows.

Configuring the Language Settings in Mozilla

Complete the following procedure to set the preferred language setting to Japanese in Mozilla.

1. Select **Edit->Preferences**. The **Preferences** window appears.
2. In the **Category** list on the left, select and open the **Navigator** dropdown list and select **Languages**. The **Languages** view appears on the right.
3. Click **Add**. The **Add Languages** window appears.
4. Select **Japanese** from the list.
5. Click **OK** to add it to the language preferences list.
6. Select **Japanese** in the language preferences list and click **Move Up** until it is at the top of the list, or select and remove any other languages listed here.
7. Click **OK** to save preferences and close the window.

Configuring the Language or Locale Settings in Windows

To have HP SIM installed and running in Japanese mode, you must set the **Locale** for the current user to **Japanese**. Refer to “Configuring Windows XP Language Settings” or “Configuring Windows 2000 Locale Settings” for more information. After you have completed these steps, install HP SIM and it will run in Japanese language mode. Refer to the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information on installing HP SIM.

Configuring Windows XP Language Settings

1. Click **Start->Control Panel->Regional and Language Options->Advanced**.
2. Under **Language to use for non-unicode programs**, select **Japanese**.
3. Click **Apply** to apply changes.
4. Reboot the system.

After rebooting the system, open a command prompt window and execute the **chcp 932** (Japanese) and **chcp 437** (English) to toggle between the two languages. The HP SIM CLI commands use the Code page to determine what locale and encoding to output, as do the Command Prompt commands, such as **dir**.

Configuring Windows 2000 Locale Settings

1. Click **Start->Settings->Control Panel->Regional Options->General**.
2. Click **Set default**. The **Select System Locale** window appears.
3. From the dropdown list, select **Japanese**.
4. Click **OK**.
5. Click **Apply**.
6. Click **Apply** to apply changes.

7. Reboot the system.

After rebooting the system, open a command prompt window and execute the `chcp 932` (Japanese) and `chcp 437` (English) to toggle between the two languages. The HP SIM CLI commands use the Code page to determine what locale and encoding to output, as do the Command Prompt commands, such as `dir`.

Configuring HP-UX and Linux Language Settings

Ensure that support for the desired languages and character map encodings are installed on the managed systems (for SSA tools) and execution system (for MSA tools, usually the CMS). To verify this, execute:

```
locale -a
```

to see if the language and character map encodings you need are listed. Furthermore, if you want to run command tools of the *x-window* command type, you must make sure that the X Display you select to display the X-Window application has been configured to use the font lists required for that application and for the requested language. For Motif X Window applications (X clients), it might be enough to just have the CDE Desktop configured for the language you want to display, it should have all the X11 resource file properties for X11 Motif or Gnome widget set font lists configured with fonts that support the language and encoding you want to use (for example, Japanese and SJIS) or you must configure the X resource file of your X clients to set the specific font lists you want to use for each application. This usually means running `xlsfonts` to find out what fonts are installed, knowing what languages the X application supports, seeing how the application sets fonts in its `app-defaults` file, and then edit the X Resource file properties on the X clients to configure the application font list properties.

Configuring HP SIM

HP SIM has a configuration file that can be modified to override locale settings that control:

- **CMS Locale.** The locale of the CMS, which affects the language used in the CMS logs and in e-mails sent by Automatic Event Handling tasks.
- **Target Locale.** The locale, character map encoding, code page, and LANG variables used when executing a command on a remote system through SSH.

This configuration file is `globalsettings.props` and is located:

- **On Windows.** It is located at `C:\Program Files\HP\System Insight Manager\config\globalsettings.props`.
- **On HP-UX and Linux.** It is located at `/etc/opt/mx/config/globalsettings.props`.

CMS Locale

By default, the CMS Locale is determined by the environment. On an HP-UX CMS, it looks for "LANG=" in `/etc/rc.config.d/LANG` and uses that setting. On a Linux CMS, it looks for "LANG=" in `/etc/sysconfig/i18n` and `/etc/sysconfig/language` and uses that setting. On a Windows CMS, it uses the default locale setting of the Java Virtual Machine, which is based on the locale setting of the user account used to install HP SIM.

If the locale used by the CMS is not the desired locale, you can manually edit `globalsettings.props` and add a line, such as `CMSLocale=en_US`, or whatever locale you want to override the CMS locale.

Target Locale

For HP SIM, the character map encoding for a locale might be different for each target operating system and each language. To allow the HP SIM to select the encoding to use for each target system (for SSA tools) or each execution system (for MSA tools, usually the CMS), we have defined the format of some properties that can be added to the `globalsettings.props` file. These properties provide the character map encoding to use for each language on each operating system, what Code Page code to use for each language on a Windows target and execution system, and the string that defines that encoding in the `LANG` environment variable on a Linux or HP-UX system. There are also properties that define what to use for unsupported languages on each operating system. The format of the property names are:

```
"TargetCharacterMapEncoding_" + language + "_" + os_name + "=" + encoding
"TargetCodePage_" + language or encoding + "_" + os_name + "=" + code
page number "TargetLangEncoding" + encoding + "_" + os_name + "=" +
encoding string
```

where *language* is the two-character code for a language, *os_name* is the upper-case keyword for the supported operating system (for example, LINUX, HPUX, WINNT), and *encoding* is the canonical name for character map encoding for that language on the operating system. The supported names can be found in column 2 of the Web page <http://java.sun.com/j2se/1.4.2/docs/guide/intl/encoding.doc.html>.

The entries look like:

```
TargetCharacterMapEncoding_ja_LINUX=EUC_JP
TargetCharacterMapEncoding_??_LINUX=ISO8859_1-
TargetCharacterMapEncoding_ja_HPUX=SJIS
TargetCharacterMapEncoding_??_HPUX=ISO8859_1
TargetCharacterMapEncoding_ja_WINNT=SJIS
TargetCharacterMapEncoding_??_WINNT=ISO8859_1
TargetCodePage_ja_WINNT=932
TargetCodePage_??_WINNT=437
```

For the Windows target and execution systems, these properties are used to choose the **chcp** command to execute in the SSH command prompt shell, to force the language and encoding to set to execute the Windows command line command. For example:

chcp 932 (forces the language to Japanese Shift-JIS)

chcp 437 (forces the language to US English with at least ISO-8859-1 support)

For Linux and HP-UX target and execution systems, the encoding is used with the locale to define the `LANG` environment variable to be defined in the SSH environment on the target and execution

systems. Example values can be found by executing the `locale -a` command on these operating systems. For example:

```
LANG=en_US.iso88591
```

(US English language, ISO-8859-1 encoding on HP-UX)

```
LANG=ja_JP.SJIS
```

(Japanese language, Shift-JIS encoding on HP-UX)

```
LANG=ja_JP.eucjp
```

(Japanese language, EUC-JP encoding on Linux)

```
LANG=en_US.utf8
```

(US English language, UTF-8 encoding on Linux)

Using Command Line Interface Commands

HP Systems Insight Manager (HP SIM) provides a command line interface (CLI) in addition to the graphical user interface (GUI). Many functions available in the GUI are also available through the CLI. This topic provides a list of the HP SIM commands available, a brief explanation of the command functionality, and a link to the associated manpages.

HP SIM Commands

HP SIM commands are installed in the following locations on the CMS:

- For HP-UX and Linux:

```
/opt/mx/bin/
```

- For Windows:

```
C:\Program Files\HP\System Insight Manager\bin\
```

Note:



The Windows path will vary if HP SIM was not installed in the default location.

To view the manpages from the command line on an HP-UX and Linux use the following manpage sections:

- For HP-UX:
 - Commands manpages are section 1M.
 - Commands that are using XML *file* manpages are section 4.

- For Linux:
 - Command that are using XML file manpages are section 4.
- For Windows:
 - Manpages are found in the following folder on Windows systems:

HP\System Insight
 Manager\hpwebadmin\webapps\mxhelp\mxportal\en\manpages

The following table provides a complete list of HP SIM commands. For a detailed explanation of these commands, click the manpage link to view an associated manpage. Use your browser's back arrow to return to this page.

Command	Functionality	Available manpages
mcompile	Compiles a Simple Network Management Protocol (SNMP) Management Information Base (MIB) file into an intermediate format (.CFG) file for importing into HP SIM using the mxmib command	mcompile(1M) [man/mcompile.1m.html]
mxagentconfig	Configures the agent to work with a central management server (CMS)	mxagentconfig(1M) [man/mxagentconfig.1m.html]
mxauth	Adds, removes, or lists a toolbox-based authorization, and copies authorizations from an existing user to another user	mxauth(1M) [man/mxauth.1m.html] mxauth(4) [man/mxauth.4.html]
mxcert	Creates a new certificate, imports a signed or trusted certificate, removes a certificate, lists certificates, generates a certificate signing request, notes whether or not to require trusted certificates, upgrades certificate from HP SIM 4.x, and synchronizes public certificate with the System Management Homepage share directory	mxcert(1M) [man/mxcert.1m.html]
mxcollection	Adds, modifies, removes, and lists collections Note: <code>mxcollection</code> XML file components and tags are case sensitive.	mxcollection(1M) [man/mxcollection.1m.html]

Command	Functionality	Available manpages
mxexec	Executes HP SIM tools, with associated arguments, on specific HP SIM managed systems, as well as verifies the status of running tools and enables a full-configuration-rights user to kill or cancel a running task	mxexec(1M) [man/mxexec.1m.html]
mxgetdbinfo	Displays information about the HP Systems Insight Manager database.	mxgetdbinfo(1M) [man/mxgetdbinfo.1m.html]
mxgethostname	Prints the name of the local host in HP SIM	mxgethostname(1M) [man/mxgethostname.1m.html]
mxglobalprotocolsettings	Used to managed global protocol settings, and sets global protocol settings from XML and lists global protocol settings in detailed format or XML format	mxglobalprotocolsettings(1M) [man/mxglobalprotocolsettings.1m.html]
mxglobalsettings	Used to manage the global settings in the <code>globalsettings.props</code> file	mxglobalsettings(1M) [man/mxglobalsettings.1m.html]
mxinitconfig	Performs initial configuration for the CMS	mxinitconfig(1M) [man/mxinitconfig.1m.html] mxinitconfig(4) [man/mxinitconfig.4.html]
mxlog	Logs an entry to the log file or standard out.	mxlog(1M) [man/mxlog.1m.html]
mxmib	Adds, deletes, and processes a list of MIBs for HP SIM and lists registered MIBs and traps for a specific registered MIB	mxmib(1M) [man/mxmib.1m.html]
mxngroup	Adds, modifies, removes, or lists system groups from HP SIM, and adds and removes systems from system list, and copies systems from one system group to another	mxngroup(1M) [man/mxngroup.1m.html] mxngroup(4) [man/mxngroup.4.html]
mxnode	Adds, modifies, identifies, removes, or lists systems in the HP SIM management domain	mxnode(1M) [man/mxnode.1m.html] mxnode(4) [man/mxnode.4.html]
mxnodesecurity	Adds, modifies, or removes security credentials for SNMP and Web-Based Enterprise Management (WBEM) protocols	mxnodesecurity(1M) [man/mxnodesecurity.1m.html]

Command	Functionality	Available manpages
mxoracleconfig	Configures HP SIM to use a newly created Oracle database after validating that HP SIM can connect to the Oracle database using the provided hostname for the Oracle server, port number of the Oracle database listener, database name, user name, password, and location of the oracle thin driver jar file. This command should be executed after the Oracle database administrator creates an instance of an Oracle database set to use Unicode (AL32UTF8) character set for exclusive use by HP SIM and provides a user name and password to access the database after granting database administrator rights to the user name. The NSL Length setting of BYTE must be used.	mxoracleconfig(1M) [man/mxoracleconfig.1m.html]
mxpassword	Adds, lists, modifies, or removes passwords stored in HP SIM	mxpassword(1M) [man/mxpassword.1m.html]
mxquery	Adds, lists, modifies, or removes lists in HP SIM	mxquery(1M) [man/mxquery.1m.html] mxquery(4) [man/mxquery.4.html]
mxreport	Lists report types, categories, and generates default and generic reports	mxreport(1M) [man/mxreport.1m.html]
mxstart	Starts daemons or processes used by the CMS	mxstart(1M) [man/mxstart.1m.html]
mxstm	Adds, removes, and lists System Type Manager rules	mxstm(1M) [man/mxstm.1m.html]
mxstop	Stops daemons or processes used by the CMS	mxstop(1M) [man/mxstop.1m.html]
mxtask	Lists, executes, removes, creates, and changes ownership for the HP SIM scheduled tasks	mxtask(1M) [man/mxtask.1m.html] mxtask(4) [man/mxtask.4.html]
mxtool	Adds, modifies, and removes tools from HP SIM	mxtool(1M) [man/mxtool.1m.html] mxtool(4) [man/mxtool.4.html]

Command	Functionality	Available manpages
mxtoolbox	Adds, modifies, or removes toolboxes from the HP SIM system	mxtoolbox(1M) [man/mxtoolbox.1m.html] mxtoolbox(4) [man/mxtoolbox.4.html]
mxuser	Adds, modifies, removes, or lists users in HP SIM	mxuser(1M) [man/mxuser.1m.html] mxuser(4) [man/mxuser.4.html]
mxwbemsub	Performs WBEM indication subscription functions on a set of systems, such as adding, deleting, listing, or moving subscriptions on each of the systems passed in as arguments	mxwbemsub(1M) [man/mxwbemsub.1m.html]

Related Topic

- Signing In

Resource Library

This section provides HP Systems Insight Manager (HP SIM) documentation links to help you perform tasks, troubleshoot problems, learn more about various features, and more!

- **Automating Software Maintenance in an HP Environment**

Refer to the Automating Software Maintenance in an HP Environment white paper at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

- **Changing the HP SIM system name**

Refer to the Changing the HP Systems Insight Manager system name white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Compiling and Customizing SNMP MIBs with HP SIM.**

Refer to the Compiling and customizing SNMP MIBs with HP Systems Insight Manager white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Configuring or Repairing Agents**

Refer to Configure or Repair Agents Online Help at <http://h18000.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Deploying HP SIM on MSCS Clusters**

Refer to the Deploying HP Systems Insight Manager on MSCS Clusters white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Installing the System Management Homepage individually (without using HP SIM)**

Refer to the System Management Homepage Installation Guide at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

- **Installing version control individually (without using HP SIM)**

Refer to the HP Version Control Installation Guide at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

- **Installing and using the HP ProLiant Essentials Performance Management Pack Data Migration Tool**

Refer to the HP ProLiant Essentials Performance Management Pack Data Migration Tool Installation and User Guide at <http://www.hp.com/products/pmp>.

- **Installing HP SIM.**

Refer to the HP Systems Insight Manager Installation and User Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Learning more about the ProLiant or Integrity Support Packs**

- To read about the ProLiant Support Pack, refer to <http://h18013.www1.hp.com/manage/psp.html>.
- To download the ProLiant Support Pack, refer to <http://www.hp.com/servers/swdrivers>.
- To download the Integrity Support Pack, refer to <http://www.hp.com/support/itaniumservers>.

- **Learning more about the ProLiant Remote Deployment Utility**

To read about the ProLiant Remote Deployment Utility, refer to <http://h18013.www1.hp.com/manage/rdu.html>.

- **Managing WBEM Event Subscriptions for HP-UX Systems with HP SIM**

Refer to the WBEM Subscriptions in HP Systems Insight Manager white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Managing HP servers through firewalls with HP SIM**

Refer to the Managing HP servers through firewalls with HP SIM white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Manually Migrating to HP SIM**

Refer to the Manually Migrating to HP Systems Insight Manager white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Moving HP SIM to a new system**

Refer to the Moving HP Systems Insight Manager to a new system white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Receiving HP driver, support, and security alerts, plus software updates customized to your HP products**

Refer to <http://www.hp.com/go/subscribe-gate1>.

- **Setting up managed systems**

Refer to “Setting Up Managed Systems”.

- **Transitioning to HP SIM**

Refer to the Transitioning to HP Systems Insight Manager white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Understanding HP SIM Security**

Refer to the Understanding HP Systems Insight Manager Security white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Using the HP ProLiant Essentials Server Migration Pack.**

Refer to the HP ProLiant Essentials Server Migration Pack User Guide at <http://www.hp.com/products/pmp>.

- **Using Secure Shell (SSH) in HP SIM**

Refer to the Secure Shell (SSH) in HP Systems Insight Manager white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Using HP OpenView**

Refer to the HP Systems Insight Manager and HP OpenView white paper at <http://h18000.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Using HP SIM with HP StorageWorks Management Software**

Refer to the Using HP Systems Insight Manager with HP StorageWorks Management Software white paper at <http://h200001.www2.hp.com/bc/docs/support/SupportManual/c00057439/c00057439.pdf>.

- **Viewing the entire HP SIM Online Help System in a PDF**

Refer to the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Viewing the HP SIM Read Me file online**

Refer to the HP Systems Insight Manager Read Me at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Viewing the entire System Management Homepage Online Help in a PDF**

Refer to the System Management Homepage Online Help at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

- **Viewing the entire HP Version Control Agent Online Help in a PDF**

Refer to the HP Version Control Agent Online Help at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

- **Viewing the entire HP Version Control Repository Manager Online Help in a PDF**

Refer to the HP Version Control Repository Manager Online Help at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

Related Topics

- Troubleshooting
- Getting Started
- Partner Applications

Discovery and Identification

Any type of discovery can only be performed if you have full-configuration-rights.

There are two types of discovery:

- **Automatic discovery.** The process that HP Systems Insight Manager (HP SIM) uses to find and identify the systems on your network and populate the database with that information. A system must first be discovered to collect data and track system health status.
- **Manual discovery.** The process that enables you to bypass a full automatic discovery and add single or multiple systems to the database, create or import the HP SIM database hosts file, and create or import a generic hosts file.

Automatic Discovery

A system must first be discovered to collect data and track system status. The **Automatically discover a system when an event is received from it** feature is disabled by default and can be enabled by selecting it in the **General Settings** section. **Automatically discover a system when an event is received from it** does not support IPX-based SNMP traps. You must enable the default **System Automatic Discovery** process for discovery to run. Go to **Options->Discovery**, select the default task and click **Enable**. It is suggested to edit this task as well to ensure the IP range is correct.

To access the **General Settings** section, select **Options->Discovery**, select the **Automatic** tab, and then click **Configure general settings**, click **Automatic** in the **Do this now to finish the installation** section of the introductory page, or click **discovery** in the **Manage** section of the **Home** page.

HP SIM performs automatic discovery using the Internet Protocol (IP) and Internetwork Packet Exchange (IPX) (Windows only) protocols.

Note:



You must enable the default **System Automatic Discovery** task for discovery to run. Select **Options->Discovery**, and select **System Automatic Discovery** task. Click **Enable**, to enable this task. HP suggests that you edit the task and verify that the IP range is correct.

IP Protocol

HP SIM discovers systems running the IP protocol when it pings systems in a listed range of addresses. It defaults to the local subnet, a range that corresponds to the IP addresses assigned to the system where HP SIM is running. You can change the address list to indicate other systems or segments of the network you want HP SIM to discover.

Web agents are not discovered unless HTTP is enabled on the **Global Protocol Settings** page in the **HTTP settings (default)** section. To enable HTTP, refer to "Setting Global Protocols" for information. To ensure that clusters are discovered in auto-discovery, **IP range pinging** must be selected in the **Configuration** section and the cluster IP address and all node addresses must be

listed in the **Ping inclusion ranges, templates and/or hosts files** section. To access the **Configuration** section, select the **Automatic** tab and click **New** for a new discovery task or click **Edit** to edit an existing discovery task.

HP SIM uses a globally unique system identifier to help identify HP systems with multiple IP addresses.

IPX Protocol

HP SIM discovers systems running the IPX protocol by listening for Service Advertising Protocol (SAP) broadcasts generated by IPX systems. Novell NetWare 3.x servers automatically make SAP broadcasts. Novell NetWare 4.x or later servers can be configured to make SAP broadcasts.

Note:



IPX is only supported on a Windows-based central management server (CMS) system and only discovers NetWare servers.

The following conditions are unique with the IPX protocol:

- IPX discovery only discovers one Network Interface Card (NIC) per machine.
- IPX systems only discover NetWare servers.

Event Based Auto-Discovery

Event based auto-discovery is disabled by default. You can enable this feature by selecting **Automatically discover a system when an event is received from it**. If selected, event based auto-discovery adds any systems that send SNMP traps, WBEM indications, or other events to HP SIM that do not have a matching IP address in the database. The **Ping exclusion ranges, templates, and/or hosts files** option allows the entry of any IP addresses that you want excluded from event based auto-discovery. If SNMP is disabled on the **Global Protocols Settings** page under **Options->Protocol Settings->Global Protocol Settings**, then SNMP traps are ignored. If WBEM is disabled, then WBEM indications are also ignored.

Note:



SNMP Authentication Failure traps do not trigger an automatic discovery. However, any other trap will do so.

Auto-discovery is disabled by default, but you can enable discovery from the **Discovery** page by selecting the **Automatic** tab, and then selecting the **System Automatic Discovery** task in the table and clicking **Enable**. Alternatively, you can click **Edit**. In the **Schedule** section, select **Automatically execute discovery every:** and set the discovery time. If you disable automatic discovery, no new automatic discovery is performed until you enable it by visiting the **Discovery** page and making your selections. You can also perform a manual discovery any time that you

choose. Refer to “Configuring Automatic Discovery” for more information on scheduling automatic discovery.

Discovery Templates

Discovery templates are files that can be used by automatic discovery in lieu of typing the addresses directly in to the **Ping inclusion ranges, templates and/or hosts files** or **Ping exclusion ranges, templates and/or hosts files** fields. They are designed to be used as a quick way to change the scope of automatic discovery. To access the discovery template section, select the **Automatic** tab from the **Discovery** page and then click **Manage templates**.

For example, you can configure a discovery template with a broad range of addresses that are discovered infrequently when you want to issue a broad range ping. When needed, the template can be used as input in the **Ping inclusion ranges, templates and/or hosts files** field of the **Edit Discovery** section. To access this section, select **Options->Discovery**, select the **Automatic** tab and then click **Edit**. The templates also enable you to quickly change the scope of discovery without having to cut and paste addresses or manually re-enter the ranges.

After creating a discovery template, to reference it in automatic discovery use `@template_name` in the **Ping inclusion ranges, templates and/or hosts files** or **Exclusion ranges, templates and/or hosts files** fields. Refer to “IP Ranges” for more information.

Note:



Since discovery now supports multiple schedules and configurations (ranges), the need for templates is significantly reduced. It is suggested to leverage several different discovery schedules and configurations instead of utilizing discovery templates.

Note:



A single discovery template cannot include both included and excluded ranges. You must create a separate template for use in each field of automatic discovery. Template files cannot be nested, that is, a template file cannot contain another template file name through the `@template_name` reference.

The format of a discovery template is the same as that used in the **Ping inclusion ranges, templates and/or hosts files** and **Ping exclusion ranges, templates and/or hosts files** fields when configuring automatic discovery.

Access discovery templates, by clicking **Manage templates** under the **For all automatic discoveries** section on the **Discovery** page. Refer to “Managing Discovery Templates” for information on creating a discovery template file.

Hosts Files

Use an existing hosts file, a file created from the HP SIM database, or an HP SIM exported hosts file as the basis for adding systems. Typically, the file is a listing of the names of systems, their IP addresses, and any alias names that are used on the system.

Importing the hosts file bypasses the need for an immediate discovery. For example, in the case of a catastrophic system failure, you could import a backup hosts file as the basis for reconfiguring your management environment and automatically repopulating the database. Adding the systems using the hosts file utility does not replace systems in the database. For example, if a system listed in the hosts file has the same IP address as an existing system, the duplicate is ignored. Any systems that previously existed in the database are not modified.

You can import hosts files from the following sources:

- The HP SIM database, which imports the system data, creates a hosts file, and sorts the data types according to your selection
- Another system that has an existing hosts file

Select the **Hosts Files** tab on the **Discovery** page to create and manage hosts files.

First Discovery

You can start a discovery in several ways:

- Execute discovery immediately from the **Discovery->Automatic** page, select the discovery task, click **Edit** to configure the discovery task for your environment, and then click **Run Now**. The discovery process starts immediately. The discovery progress is updated as the systems are discovered, until the discovery process is complete.
- Allow sufficient time for a complete discovery and identification to finish. Times vary, depending on your network, bandwidth, and discovery settings. In most cases, the discovery process finds all systems by pinging the network.

Subsequent Discoveries

You can run discovery at any time from the **Discovery->Automatic** page. For subsequent discoveries, you can specify which subnets or systems to interrogate, which protocols to use, and which schedule to follow. Select IPX as a discovery protocol if your network includes Novell systems.

For the most comprehensive discovery and identification, always select SNMP, DMI, WBEM, and HTTP as the protocols on the **Options->Protocol Settings->Global Protocol Settings** page. Configure default community strings and WBEM passwords on the **Global Protocol Settings** page. Refer to "Global Protocols" for additional information.

Status indicators indicate when discovery is running, and the column, **Last Run**, displays **running**, the percent complete, and the number of **pings attempted** and systems **processed** are displayed. A processed system is one whose IP address has been identified or found to be unresponsive. A processed system is not necessarily added to the database.

Manual Discovery

Manual discovery enables you to bypass a full discovery. With manual discovery, you can:

- Add a single system to the HP SIM database
- Add multiple systems through hosts files

- Create and import an HP SIM hosts file
- Import a hosts file that was created or exported from Insight Manager (WIN32) (the hosts file automates the process of adding systems or restoring system information)
- Create or import a generic hosts file to automate the process of adding systems or restoring system information
- Set up systems before they are physically on the network

The system is added to the database with the IP address as the system name. After the system is up on the network and identification runs, the system name is updated with the system name instead of IP address.

You can access the manual discovery page by:

- Clicking **Options->Discovery** and selecting the **Manual** tab
- Clicking **Manual** in the **Do this now to finish the install** section of the introductory page
- Clicking **discovery** in the **Manage** section of the **Home** page

Options for Adding a Single System

- Know the IP address or hostname of the system. If you know at least one of these, HP SIM can find the other by validating the information with the Domain Name Service (DNS) for the network.
- To add a cluster and its nodes, enter each IP address separately.
- Decide if you want to set the system type, subtypes, or WBEM credentials as well as the product model.
- Specify the **WBEM Settings** for the system on the **System Protocol Settings** page. You can override the default user name and passwords by selecting the use custom settings and entering appropriate user names and passwords.
- Specify the SNMP settings for this system to be unique or match the global discovery settings. The current system default settings are displayed. If you override the default and specify a different value, that community string must be supported on the system. If it is not, and one of the defaults is supported, then HP SIM reverts back to the default value. You can modify the following settings:

<p>timeout</p>	<p>The amount of time HP SIM waits for an SNMP response when it sends a request to the system. The default timeout value appears. If a response is not received within the time interval, HP SIM might determine that the system does not support SNMP. Decreasing this value can result in increased network traffic because the number of attempts is accelerated. Use caution when changing this value. A value of three seconds usually works for a LAN. However, If systems are connected through a WAN, try a higher value, for example, ten seconds.</p>
----------------	---

retries	The number of additional times after the first attempt is made to communicate with a system before attempts stop.
community strings	A community string sets up authentication that enables or prohibits communication between the system and the console. The community string of the console must match the community string of the system. Use the read-only community string to read variables. Use the write community string to modify variables. Although only one community is valid for a communication attempt, a system can belong to multiple communities. However, HP SIM only uses one community string when communicating to a system.

Note:



If an IP address is used, it must be properly resolved to a name for the name to be displayed in the GUI.

Refer to “Adding a System Manually” for the steps to add a single system to the database.

Related Procedures

- Configuring Automatic Discovery
- Configuring Discovery General Settings
- Creating a New Discovery Task
- Editing a Discovery Task
- Disabling or Enabling a Discovery Task
- Deleting a Discovery Task
- Running a Discovery Task
- Creating a New Discovery Template File
- Editing a Discovery Template
- Deleting a Discovery Template
- Adding a System Manually
- Creating a New Hosts File
- Editing a Hosts File
- Deleting a Hosts File
- Adding Systems in a Hosts File to the Database

Related Topics

- Managing Hosts Files
- Managing Discovery Templates
- Identification
- Discovery Filters
- Data Collection
- Status Polling

- Protocols
- Discovery and Identification

Configuring Automatic Discovery

When accessing the **Automatic** tab on the **Discovery** page, a table displays a listing of all available discovery tasks. You can configure multiple instances of discovery with each instance having its own schedule and set of inclusion ranges. When a discovery task is executed, the **Last Run** column is updated to display its progress, including the percentage complete.

Note:



There are two parts to automatic discovery and percent complete, and it is calculated by weighting two factors. First, there is a ping sweep on each host, which counts as 10% of the process. Second, the identification process counts as 90% of the process. (If no host was found on that IP, the 90% part is considered complete.) For example, if you have 100 hosts in your discovery range and 50 have been pinged, but only 10 have been identified, you have: $50/100 * .10 = 0.05$ (ping sweep) $10/100 * .90 = 0.09$ (identification) $0.05 + 0.09 = 0.14 * 100 = 14\%$ (total completed percentage).

Note:



Only one discovery task can run at a time. If you select to run more than one discovery task, the percentage in the **Last Run** column remains at 0% until the currently running task is complete.

Under the **For all automatic discoveries** section, there are three options available:

- **Configure general settings.** Used to configure settings that apply to all discovery tasks. Refer to “Configuring Discovery General Settings” for more information.
- **Manage templates.** Used to manage discovery templates. Refer to “Managing Discovery Templates” for more information.
- **Configure global protocol settings.** Used to configure global protocol settings. Refer to “Setting Global Protocols” for more information.

Note: Simple Network Management Protocol (SNMP) must be enabled with correct security settings on HP Systems Insight Manager (HP SIM) and running on the target systems to discover clusters correctly.

Note: DMI identification is only supported on Windows and HP-UX-based central management server (CMS) installs. In addition, only like operating systems can be identified. For example, Windows-based CMSs can identify Windows-based DMI, and HP-UX-based CMSs can only identify HP-UX-based DMI systems.

Also from the **Automatic** tab, you can:

- **Create a new discovery task.** Click **New** and the **New Discovery** section appears. Refer to “Creating a New Discovery Task” for more information.
- **Edit an existing discovery task.** Select a task from the table and click **Edit**. The **Edit Discovery** section appears. Refer to “Editing a Discovery Task” for more information.
- **Enable or disable a discovery task.** Select a task and click **Disable** to disable the schedule of an enabled task. If a task is disabled, the button changes to **Enable** and to resume automatic execution of the task, click **Enable**. Refer to “Disabling or Enabling a Discovery Task” for more information.
- **Delete an existing discovery task.** Select a task from the table and click **Delete**. Refer to “Deleting a Discovery Task” for more information.
- **Run a discovery task.** Select the task you want to run and click **Run Now**. When a task is running, the **Run Now** button changes to a **Stop** button. Refer to “Running a Discovery Task” for more information.

Note:



Two discovery tasks cannot be running at the same exact time, instead the second task displays 0% until the first task completes.

- **Stop a discovery task from running.** Select the running task and click **Stop**. Refer to “Running a Discovery Task” for more information.
- **View HP Storage Essentials discovery status.** When HP Storage Essentials is installed, its discovery status is displayed with a link to the HP Storage Essentials discovery log.
- **Configure HP Storage Essentials global application settings.** When HP Storage Essentials is installed, the **Automatic** tab includes a link to the HP Storage Essentials global application settings configuration page.

Related Procedures

- Configuring Discovery General Settings
- Creating a New Discovery Task
- Editing a Discovery Task
- Disabling or Enabling a Discovery Task
- Deleting a Discovery Task
- Running a Discovery Task
- Creating a New Discovery Template File
- Editing a Discovery Template
- Deleting a Discovery Template
- Setting Global Protocols

Related Topics

- Discovery and Identification
- Managing Discovery Templates

- IP Ranges

Creating a New Discovery Task

This procedure enables you to create new discovery tasks.

1. Select **Options->Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. Click **New** to create a new discovery task. The **New Discovery** section appears.

New Discovery

Required field *

Name: *

Schedule:

Automatically execute discovery every:

days AM

Configuration:

IPX SAP

IP range ping

Ping inclusion ranges, templates, and/or hosts files: *

3. In the **Name** field, enter a name for the task. This is a required field.
4. In the **Schedule** section, select **Automatically execute discovery every** and enter when the task should run. The default is one a day. If you deselect **Automatically execute discovery every**, the task is disabled after it is created.
5. In the **Configuration** section, select from:
 - IP range ping
 - IPX SAP (Windows CMS only)
6. In the **Ping inclusion ranges, templates and/or hosts files** field, specify the IP addresses to include for pinging. Refer to "IP Ranges" for more information on entering IP ranges.
7. Click **OK** to save the task, or **Cancel** to close the **New Discovery** section and not save any settings.

Note: If you have selected a large number of systems, a message appears, stating The automatic discovery task is configured with a large number of addresses: [NUM]. Click **OK** to continue anyway or click **Cancel** to change the IP address range.

Related Procedures

- Configuring Discovery General Settings
- Editing a Discovery Task
- Disabling or Enabling a Discovery Task

- Deleting a Discovery Task
- Running a Discovery Task

Related Topics

- Discovery and Identification
- IP Ranges

Editing a Discovery Task

When editing an existing discovery task, all fields are pre-populated with existing information. Only edit the fields that you want to edit.

To edit an existing discovery task:

1. Select **Options->Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. Select the task to be edited and click **Edit**. The **Edit Discovery** section appears.
3. In the **Name** field, enter a name for the task. This is a required field.
4. In the **Schedule** section, select **Automatically execute discovery every** and enter when the task should run. The default is one a day. If you deselect **Automatically execute discovery every**, the task is disabled after it is created.
5. In the **Configuration** section, select from:
 - **IP range pinging**
 - **IPX SAP (Windows only)**
6. In the **Ping inclusion ranges, templates and/or hosts files** field, specify the IP addresses to include for pinging. Refer to "IP Ranges" for more information on entering IP ranges.
7. Click **OK** to save the task, or **Cancel** to close the **New Discovery** section and not save any settings.

Note: If you have selected a large number of systems, a message appears, stating `The automatic discovery task is configured with a large number of addresses: [NUM]`. Click **OK** to continue anyway or click **Cancel** to change the IP address range.

Related Procedures

- Configuring Discovery General Settings
- Creating a New Discovery Task
- Disabling or Enabling a Discovery Task
- Deleting a Discovery Task
- Running a Discovery Task

Related Topics

- Discovery and Identification
- IP Ranges

Disabling or Enabling a Discovery Task

You can disable or enable an existing discovery task. If you disable a task, the **Schedule** column displays a message stating that the task is disabled. If a task is enabled, the **Schedule** column displays the schedule for the task.

Note:



Manually running a disabled task by selecting the task and clicking **Run Now** does not enable the task for future discoveries.

To disable or enable a discovery task:

1. Select **Options->Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. Select the task to disable or enable.
3. Click **Disable** to disable a task, or if the task is already disabled, click **Enable** to resume the automatic execution of a task.

Related Procedures

- Configuring Discovery General Settings
- Creating a New Discovery Task
- Editing a Discovery Task
- Deleting a Discovery Task
- Running a Discovery Task

Related Topic

- Discovery and Identification

Deleting a Discovery Task

You can delete discovery tasks that are no longer needed. You cannot delete the **Default Discovery** task. If you select the **Default Discovery** task, the **Delete** button is disabled.

To delete a discovery task:

1. Select **Options->Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. Select the tasks to delete and click **Delete**. A confirmation box appears.
3. Click **OK** to delete the task, or click **Cancel** to cancel the deletion process.

Related Procedures

- Configuring Discovery General Settings
- Creating a New Discovery Task
- Editing a Discovery Task

- Disabling or Enabling a Discovery Task
- Running a Discovery Task

Related Topics

- Discovery and Identification
- IP Ranges

Running a Discovery Task

You can manually select and run any existing discovery task at any time. You can also stop a task that is running.

To run or stop a discovery task:

1. Select **Options->Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. Select the discovery task that you want to run and click **Run Now**. The task runs immediately.

Note:



The **Run Now** button changes to **Stop** when a task is running. To stop a task, select the task and click **Stop**.

Related Procedures

- Configuring Discovery General Settings
- Creating a New Discovery Task
- Editing a Discovery Task
- Disabling or Enabling a Discovery Task
- Deleting a Discovery Task

Related Topics

- Discovery and Identification
- IP Ranges

System Types

There are many different system types in HP Systems Insight Manager (HP SIM). All of these are available on the **Discovery Filters** page, except clusters, complex, racks, and enclosures.

- **Application.**
- **Cluster.** A virtual computer usually made up of several servers clustered together with special software. Clusters are typically a fault-tolerant configuration. If a system is expected to be a cluster, but not identified as such, be sure that the agents are properly configured on the cluster nodes and that it is a supported cluster environment.

- **Complex.** Computer systems that support multiple hardware partitions are referred to as a complex. For example, the HP Integrity Superdome class systems support multiple hardware partitions within a single complex.
- **Desktop.** A small computer system typically located on users desks.
- **Enclosure.** A chassis that can hold server blades and other types of blades. Many times, enclosures are not connected to a network but can provide power and cooling to the blades installed in them.
- **Environmental Monitor.** A device that monitors the environment around a system, rack, or so on. It checks for temperature, smoke, and security.
- **Handheld.** A Personal Digital Assistant (PDA) or small computer that fits in your hand.
- **Hub.** Also called a repeater, a simple device typically used to extend the number of ports available on the network.
- **KVM switch.** A keyboard, video, and mouse switch used to enable a single keyboard, video monitor, and mouse to be shared by multiple systems, which can be network enabled.
- **Management Processor.** Usually a small firmware-based system that is embedded in a server or other server related hardware such as an enclosure. These systems are typically limited in their capabilities, one example would be the Integrated Lights-Out (iLO) card.
- **Notebook.** A portable computer.
- **Partition.** Certain systems and operating environments can be flexibly configured into partitions, each of which can run a separate instance of the operating system. Partitions provide protection that prevents software errors in one partition from interfering with another partition. Further, server systems that allow for hardware partitions can protect hardware errors from interfering with another partition.
- **Power Distribution Unit.** Provides power to multiple systems in a rack, which can be remotely controlled to enable the powering on or off of a given system.
- **Power supply.** A device that supplies power for servers on your network.
- **Printer.** A device that is used to print on paper, which is typically attached to the network as well.
- **Rack.** A non-addressable piece of hardware used to mount servers, enclosures, or networking equipment.
- **Resource Partition.**
- **Remote Access Device.** A device to allow remote users to dial in through a phone line or over the LAN to an intranet.
- **Router.** A networking device used to route network packets.
- **Server.** A computer on a network that is dedicated to a particular purpose. For example, a file, print, or database server.
- **Shared Resource Domain.**
- **Storage Device.** A disk drive array.

- **Switch.** A network device, similar to a router but uses hardware-based switching technology to route packets in very fast manner.
- **Tape library.** A tape library.
- **Thin client.** A remote system connecting to a terminal server, a computer that has no disk or local storage and enables you to connect through terminal server packages to a central server or remote desktop.
- **Uninterruptible Power Supply (UPS).** A battery backup for servers or other computers.
- **Unknown.** In HP SIM, a status indicating that none of the built-in or System Type Manager (STM) based tasks could identify the system. However, some management protocol was detected on the system. Servers might be listed as Unknown for the following reasons:
 - You must be able to ping the system from the server where HP SIM is running. This can be accomplished from a command or terminal window, or from HP SIM selecting the unknown server and selecting menu pull-downs Diagnose and Ping and following the steps listed.
 - Community strings in HP SIM must match the ones used for the remote device. Be sure HP SIM and the systems are using the same community string. Note that community strings are case sensitive. From HP SIM, select **Options->Protocol Settings** and select **Global Protocol Settings** or **System Protocol Settings** to make the changes.
 - Under Windows NT and Windows 2000, one community name on the system must be set to *Read Create*. Note that you do not have to use this community string in HP SIM (a community string set to *Read* is all that is required). The Management Agents connect to themselves using SNMP and require one string set to *Read Create*.
 - The HP SIM system must be allowed to make SNMP requests to the managed systems. Be sure the SNMP security settings are not preventing this. Under Windows NT and Windows 2000, the **Allow SNMP packets from any host** must be selected or the address of the HP SIM server must be in the list of allowed hosts.
 - If you are using IP-specific security, *localhost (127.0.0.1)* must also be allowed to make SNMP requests to the host. The *localhost* entry enables the Management Agents to connect to themselves using SNMP.
 - The ProLiant Management Agents must be installed and running properly on the ProLiant servers you are trying to manage. For Windows systems, check the Event Log to make absolutely sure they are running (you should see a few *Agents started* messages and no errors).
 - Routers and switches in the network must allow SNMP traffic to pass on ports 161, 162, and 7.
- **Unmanaged.** A type indicating that a system that was found with an IP address, without any detected management protocols. If this is not the expected type, ensure the WBEM user name and password or the SNMP community name is correct. Install agents if possible (for example, for Windows, install the Initial ProLiant Support Pack). Refer to "Initial ProLiant Support Pack Install" for information on installing the Initial ProLiant Support Pack.
- **Workstation.** A higher-end personal computer system, sometimes used for graphics or other design work.

Configuring Discovery General Settings

Configure automatic discovery to customize the discovery process for your environment.

Note:



All steps are optional.

To configure general settings for automatic discovery:

1. Select **Options->Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. In the **For all automatic discoveries** section, select **Configure general settings**. The **General Settings** section appears.
3. Select **Automatically discover a system when an event is received from it**. This option allows systems to be discovered when a trap or some other supported event is received by HP Systems Insight Manager (HP SIM). It uses the discovery filters and IP address exclusion ranges for additional filtering of these events.
4. Select **Automatically discover a server blade when its Integrated Lights Out management processor is identified**. This option adds servers that were indirectly discovered through its management processor. When these servers are discovered, they are listed with a Disabled state on the system table view page and the only information displayed is the system serial number and the association to the iLO and the enclosure.
5. In the **Ping exclusion ranges, templates and/or hosts files** field, specify the IP addresses, templates, or hosts files containing IP addresses to exclude from the automatic discovery process. This applies to both range pinging and event based auto-discovery. Refer to "IP Ranges" for more information.

Important: When discovering clusters, the ping inclusion range must include the IP addresses of the cluster and the cluster members.

6. Select **Enable discovery filters**.
7. In the **Discover the following system types:** section, select the type of systems to be discovered. Refer to "System Types" for more detailed information on each of the system types listed.

Important: When discovering clusters, you must include the Server system type, or so that the cluster members are not filtered out.

Note: This is only available when you select **Enable discovery filters**.

8. In the **Limit discovery to systems that meet the following criteria** section, select from the following:
 - **Any system that matches the above filter**

- **All manageable systems (WBEM, SNMP, DMI, WMI or HTTP support)**
- **Manageable systems with HP agents only**

Note: This is only available when you select **Enable discovery filters**.

9. Click **OK** to save settings, or click **Cancel** to close the **General Settings** section without saving changes.

If you click **OK** when discovery filters are enabled but have not selected any system types, the following error message appears:

```
You must make at least one system type selection when enabling filters.
```

The **Discovery** page **General Settings** section is not protected from multiple users accessing the page at the same time. The last user to save the settings has their settings take affect. If discovery is in progress and the settings are applied by a different user or the same user, any remaining systems to be processed have the settings applied.

Related Topics

- Discovery and Identification
- IP Ranges
- Discovery Filters
- System Types
- Global Protocols

Discovery Filters

Discovery filters are a mechanism to prevent or allow certain system types from ever being added to the database through automatic discovery. When you want to discover systems of certain types, using filters is much easier than the alternative of specifying the IP addresses of each individual system. Discovery filters do not apply to manually added systems.

There are three ways to access discovery filters:

- Select **Options->Discovery** to access the **Discovery** page. From the **Automatic** tab, click **Configure general settings** and select **Enable discovery filters**.
- From the **Home** page, in the **Manage** section, click **discovery**. The **Discovery** page appears. From the **Automatic** tab, click **Configure general settings**, and select **Enable discovery filters**.
- From the introductory page, in the **Do this now to complete the installation** section, click **Automatic**. The **Discovery** page appears. From the **Automatic** tab, click **Configure general settings**, and select **Enable discovery filters**.

To disable filters, deselect the **Enable discovery filters** checkbox. To enable filters, check the **Enable discovery filters** checkbox and select the appropriate system types that you want to discover.

To access and modify discovery filters, you must have full-configuration-rights. If discovery filters are enabled, only systems of the selected types are added to the database through automatic discovery. Because all tasks operate on systems that exist in the database, tasks do not run on any

system until the filter has been met and that system has been added to the database. The filters do not affect any systems already discovered, even if they change to a type that no longer matches the current filter. If discovery filters are disabled, automatic discovery discovers systems according to the **General Settings** section on the **Discovery** page, **Automatic** tab. Refer to “Configuring Discovery General Settings” for more information on configuring discovery filters.

If you do not discover the HP systems that you expect to find, ensure the HP Insight Management Agents are installed and running correctly on the target systems. In addition, verify that the SNMP Community Strings settings and WBEM user name and passwords in HP Systems Insight Manager (HP SIM) and on the agents for systems that are not discovered are configured correctly. Refer to “Setting Global Protocols” for more information.

Related Procedure

- Configuring Discovery General Settings

Related Topic

- Discovery and Identification

Managing Discovery Templates

Discovery templates are files that can be used by automatic discovery in lieu of typing the addresses directly in to the **Ping inclusion ranges, templates and/or hosts files** or **Ping exclusion ranges, templates and/or hosts files** fields. They are designed to be used as a quick way to change the scope of automatic discovery.

Note:



Saved discovery template files go into the `<install directory>\config\discovery\templates` directory.

From the **Managing Templates** section, you can:

- **Create new discovery template files.** Click **New** and the **Create New Template** section appears. Refer to “Creating a New Discovery Template File” for more information.
- **Edit existing discovery template files.** Select the discovery template file that you want to edit and click **Edit**. The **Edit Template** section appears. Refer to “Editing a Discovery Template” for more information.
- **Delete existing discovery template files.** Select the discovery template file that you want to delete and click **Delete**. A confirmation box appears. Refer to “Deleting a Discovery Template” for more information.

Related Procedures

- Creating a New Discovery Template File
- Editing a Discovery Template

- Deleting a Discovery Template

Related Topic

- Discovery and Identification

Creating a New Discovery Template File

You can create new discovery template files in lieu of typing the addresses directly in to the **Ping inclusion ranges, templates and/or hosts files** or **Ping exclusion ranges, templates and/or hosts files** fields.

To create a new discovery template file:

1. Select **Options->Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. In the **For all automatic discoveries** section, select **Manage templates**. The **Manage Templates** section appears.
3. Click **New**. The **Create New Template** section appears.
4. In the **Discovery template name** field, enter a name for the new template. This field is required.
5. Click **Browse** to select an existing discovery template file that is present on the local client (the system from which you are browsing) and click **Import**.

or

Enter the discovery range information into the **Contents** area.

Note: Template files cannot be nested, so only ranges are allowed.

6. Click **OK** to save the discovery template file, or click **Cancel** to close without saving changes.

After creating a discovery template, you can reference it in automatic discovery by using *@template_name* in the **Ping inclusion ranges, templates and/or hosts files** or **Ping exclusion ranges, templates and/or hosts files** fields. Refer to “IP Ranges” for more information.

Related Procedures

- Editing a Discovery Template
- Deleting a Discovery Template

Related Topics

- Discovery and Identification
- Managing Discovery Templates

Editing a Discovery Template

You can edit an existing discovery template file. All fields are optional except for the **Discovery template name** field. Edit only the fields that you want to change.

To edit a discovery template file:

1. Select **Options->Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. In the **For all automatic discoveries** section, select **Manage templates**. The **Manage Templates** section appears.
3. Select a discovery template file to edit and click **Edit**. The **Edit Template** section appears.
4. In the **Discovery template name** field, change the name of the template. This field is required, but you do not have to create a new name for the template. You can use the existing name.
5. Click **Browse** to select an existing discovery template file that is present on the local client (the system from which you are browsing) and click **Import**.

or

Enter the discovery range information into the **Contents** area.

Note: Template files cannot be nested, so only ranges are allowed.

6. Click **OK** to save the discovery template file, or click **Cancel** to close without saving changes.

Related Procedures

- Creating a New Discovery Template File
- Deleting a Discovery Template

Related Topics

- Discovery and Identification
- Managing Discovery Templates

Deleting a Discovery Template

You can delete existing discovery template files. If you delete a discovery template file, the file is permanently deleted and cannot be retrieved. Only delete discovery template files if you no longer need them or you are creating an new discovery template file.

Note:

Be sure this template is not currently in use. A template is not in use when:



- There are no references to it in the **Ping exclusion ranges, templates and/or hosts files** field in the **General Settings** section.
and
- There are no references to it in the **Ping inclusion ranges, templates and/or hosts files** field of all existing discovery tasks.

To delete a discovery template file:

1. Select **Options->Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. In the **For all automatic discoveries** section, select **Manage templates**. The **Manage Templates** section appears.
3. Select a discovery template file to delete.
4. Click **Delete**. A confirmation box is displayed.
5. Click **OK** to delete the discovery template file, or click **Cancel** to cancel the deletion process.

Related Procedures

- Creating a New Discovery Template File
- Editing a Discovery Template

Related Topics

- Discovery and Identification
- Managing Discovery Templates

Adding a System Manually

Use manual discovery to add a system to the HP Systems Insight Manager (HP SIM) database between scheduled discoveries.

To add a system using manual discovery:

1. Select **Options->Discovery** and select the **Manual** tab. The **System Information** section appears.
2. Select the **System name** radio button and enter the system name.

or

Select the **IP address** radio button and enter the IP address.
3. Click **Add System** to add the system to the database, or click **More Settings** to enter additional information.

System Information

Required field *

Enter either the system's name or IP address: *

System name:

IP address:

Specify additional system properties to use only if Identification fails on this system

System type:

System subtype 1:

System subtype 2:

System subtype 3:

System subtype 4:

System subtype 5:

System subtype 6:

System subtype 7:

System subtype 8:

Product model:

WBEM Settings

User name

Use default (currently:)

Use custom

Password

Use default

Use custom Verify Password

SNMP Settings

Timeout (in seconds)

Use default (currently: 5)

Use custom

Retries

Use default (currently: 1)

Use custom

Read-only community string

Use default (currently: public)

Use custom

Write community string

Use default (currently: private)

Use custom

- **Specify additional system properties to use only if Identification fails on this system.**

Includes:

- **System type**
- **System subtype**

There are eight available System subtype fields that can later be changed on **System Attributes** page. Refer to “Editing System Properties for a Single System” for more information on editing the System subtypes for one system. Refer to “Editing System Properties for Multiple Systems” for more information on editing the System subtypes for multiple systems.

- **Product model**

- **WBEM Settings.** Includes:
 - **User name**
 - **Password**

 - **SNMP Settings.** Includes:
 - **Timeout (in seconds)**
 - **Retries**
 - **Read-only community string**
 - **Write community string**
4. If you clicked **More Settings**, click **Add System** to add the system immediately or click **Fewer Settings** to return to the previous brief display. If you clicked **Fewer Settings**, click **Add System** to add the system to the database.

Hosts files can be used to manually add multiple systems to the HP SIM database. Refer to “Managing Hosts Files” for more information.

Command Line Interface

Use the **mxnode** command to perform this task from the command line interface (CLI). For assistance with this command, refer to the HP-UX or Linux manpage by entering **man mxnode** at the command line. Refer to “Using Command Line Interface Commands” for more information on the command and a link to the manpage.

Related Procedure

- Creating a New Hosts File

Related Topics

- Discovery and Identification
- IP Ranges

Managing Hosts Files

Hosts files can be used to manually add multiple systems to the HP Systems Insight Manager (HP SIM) database.

To use a hosts file to specify systems for an automatic discovery, add the hosts file name to the **Ping inclusion ranges, templates and/or hosts files** section on the **Discovery** page, **Automatic** tab, **Configure general settings**. Use the following statement: `$Hosts_filename`.

Refer to “Adding a System Manually” for information on adding a single system to the database.

From the **Hosts Files** section, you can:

- **Create new hosts files.** Click **New** and the **New Hosts File** section appears. Refer to "Creating a New Hosts File" for more information.
- **Edit a hosts file.** Select the hosts file to edit and click **Edit** and the **Edit Hosts File** section appears. Refer to "Editing a Hosts File" for more information.
- **Delete a hosts file.** Select the hosts file to delete and click **Delete**. A confirmation box appears. Refer to "Deleting a Hosts File" for more information.
- **Add a hosts file to the HP SIM database.** Select the hosts file to add and click **Add system now**. Refer to "Adding Systems in a Hosts File to the Database" for more information.

Related Procedures

- Creating a New Hosts File
- Editing a Hosts File
- Deleting a Hosts File
- Adding Systems in a Hosts File to the Database
- Creating a Task to Import a Hosts File for HP Systems Insight Manager Integration Task

Related Topic

- Discovery and Identification

Creating a New Hosts File

This procedure enables you to create a new hosts file for use in HP Systems Insight Manager (HP SIM).

Note:



For a keyword that contains more than one word, such as "management processor," enclose the full keyword in double quotation marks. Quotation marks are optional for single keywords like server.

Note:



For clusters, be sure that the cluster and its members are defined in the hosts file.

To create a hosts file:

1. Select **Options->Discovery** and select the **Hosts Files** tab.
2. Click **New** to create a new hosts file. The **New Hosts File** section appears.

New Hosts File

Required field *

Name:

Initialize contents with:

Template file

Systems loaded from the central management server, sorted by:

Systems loaded from hosts file:

Contents:

```
# Title:      [title here]
# Author:    [author here]

# Example:
##$INXE_DEFAULT: Type = server
# 1.1.1.1   myServer1.mysite.com   myServer1
# 1.1.1.2   myServer2.mysite.com   myServer2
#
##$INXE_DEFAULT: Type = desktop
# 1.1.1.3   myClient1.mysite.com    myClient1
# 1.1.1.4   myClient2.mysite.com    myClient2
```

3. In the **Hosts file name** field, enter a name for the new hosts file. This field is required.
4. Under **Initialize contents with**, select one of the following:
 - **Empty file.** Resets the contents into the **Contents** window.
 - **Systems loaded from the central management server, sorted by:.** Select the **IP address, System name, System type and then by IP address, or System type and then by System name.** This option loads the systems being managed by HP SIM into the **Contents** window.
 - **Systems loaded from hosts file.** Enter the file name and location (for example, `c:\doc.txt`) or click **Browse** to browse to the location of the hosts file. This option reads the contents of the specified file and displays it in the **Contents** window.
5. If you did not select **Empty File**, click **Initialize Now** to load the hosts file. Otherwise, enter the contents of the hosts file in the **Contents** section.
6. Click **OK** to save the hosts file, or click **Cancel** to cancel any changes you have made.

Related Procedures

- Editing a Hosts File
- Deleting a Hosts File
- Adding Systems in a Hosts File to the Database

Related Topics

- Discovery and Identification
- Managing Hosts Files

Editing a Hosts File

Perform the following procedure to edit an existing hosts file. Edit only the fields that you want.

To edit an existing hosts file:

1. Select **Options->Discovery** and select the **Hosts Files** tab.
2. Select an existing hosts file and click **Edit**. The **Edit Hosts File** section appears.
3. In the **Replace contents with** section, select one of the radio buttons and click **Replace Now**, or enter the changes in the **Contents** section. Refer to "Creating a New Hosts File", step 5 for more information on the radio buttons.
4. Click **OK** to save changes, or click **Cancel** to not save any changes.

HP Systems Insight Manager (HP SIM) reads in the hosts file and adds the systems.

Related Procedures

- Creating a New Hosts File
- Deleting a Hosts File
- Adding Systems in a Hosts File to the Database

Related Topics

- Discovery and Identification
- Managing Hosts Files

Deleting a Hosts File

Be sure that this hosts file is not in use. A hosts file is not in use when:

- There are no references to it in the **Ping exclusion ranges, templates and/or hosts files** section of the general settings page.
- There are no references to it in the **Ping inclusion ranges, templates, and/or hosts files** section of every existing discovery task.

Note:



Only delete hosts files if you no longer need them or if you are creating a new hosts file.

To delete a hosts file:

1. Select **Options->Discovery** and select the **Hosts Files** tab.
2. Select hosts files to delete and click **Delete**. A confirmation box appears.
3. Click **OK** to delete the hosts files, or click **Cancel** to cancel the delete process.

Related Procedures

- Creating a New Hosts File
- Editing a Hosts File
- Adding Systems in a Hosts File to the Database

Related Topics

- Discovery and Identification
- Managing Hosts Files

Adding Systems in a Hosts File to the Database

Perform this procedure to add hosts files to the HP Systems Insight Manager (HP SIM) database.

To add hosts files to the database:

1. Select **Options->Discovery** and select the **Hosts Files** tab.
2. Select an existing hosts file.
3. Click **Add Systems Now**.

HP SIM reads in the hosts file and adds the systems.

Related Procedures

- Creating a New Hosts File
- Editing a Hosts File
- Deleting a Hosts File

Related Topics

- Discovery and Identification
- Managing Hosts Files

Creating a Task to Import a Hosts File for HP Systems Insight Manager Integration Task

Users with full-configuration-rights who are using both HP Systems Insight Manager (HP SIM) and its companion Windows management application, Insight Manager (WIN32), can import Insight Manager (WIN32) system database files for easy transition from the Windows client server environment to the Web-based environment.

Insight Manager (WIN32) creates a system database file that stores the names and IP addresses of discovered systems in a file called `cim_ip.dat`. The file is formatted like a hosts file that HP SIM recognizes. The file is dynamically updated as systems are discovered or deleted in Insight Manager (WIN32). You can find the file in the directory where Insight Manager (WIN32) is installed.

Insight Manager (WIN32) supports systems that have spaces in their names. In the `cim_ip.dat`, these system names contain an asterisk (*) instead of the space. Any system name that contains a space is invalid in HP SIM.

Importing the .dat File

Note:



If the hosts file contains a cluster name or address, the HP SIM discovery IP range must be changed to include the cluster members since it is possible that the imported hosts file does not include the cluster members. Refer to “Creating a New Discovery Task” for information on changing the IP range.

1. Select **Options->Discovery**, then select the **Manual Discovery** tab, and click **Hosts Files** at the top of the page. The **Manual Discovery - Hosts Files** page appears.
2. Click **New**. The **New Hosts File** section appears.
3. In the **Hosts file name** field, enter a name for the file, such as **cim_ip.dat**.
4. Select **Systems loaded from hosts file** and enter the full path name for the file or locate the **cim_ip.dat** file, by clicking **Browse**. When the file is found, click **Open** to enter the file name in the **Systems loaded from hosts file** field.
5. Click **Initialize Now** to initialize the file and display the contents in the **Contents** area.
6. Click **OK** to save the file as a hosts file for future reference.
7. On the **Manual Discovery - Hosts File** page, be sure the file you added is selected, and click **Add Systems Now** to insert the systems into the database.

Displaying the Systems

Within a short time, the systems inserted through a hosts file are added to the database. When the next discovery and identification tasks run, full system information is added to the system.

In the **Systems and Events** panel, select **All Systems**. The system table view page displays, and the systems added should be displayed along with all other discovered systems.

Exporting Insight Manager (WIN32) Files

There are two ways to export Insight Manager (WIN32) .DAT files from within Insight Manager (WIN32):

- Using the Insight Manager (WIN32) Export feature
- Using the **cim_ip.dat** file, which contains abbreviated system information compared to the first method

Go to

http://h20000.www2.hp.com/bc/docs/support/UCR/SupportManual/TPM_12ky0500-wwen/TPM_12ky0500-wwen.pdf for more information on exporting the Insight Manager (WIN32) .dat file.

Related Procedure

- Managing Hosts Files

Hosts File Extensions

Hosts files typically contain IP addresses, system names, system name aliases, and user comments. The hosts file that you create can contain additional information about systems. The information appears as one or more comments that precede the hosts file entry for the system. Unless other values are specified, the default values are used. Defaults are provided for the following parameters:

Parameter	Keyword
system type	TYPE
SNMP timeouts	SNMP_TIM
SNMP retries	SNMP_RET
SNMP read community	SNMP_MON
SNMP write community	SNMP_CON

You can modify the hosts file to substitute a value for the defaults for one entry or change the default for all subsequent entries. To change values for a single system entry in a hosts file, add a statement to the hosts file as a comment on the line before the host entry as shown in the following example. The statement applies to the system it precedes and only to that system. In the following example, the default TYPE is changed to server for the system EngProliant.

Keyword Statement	Hosts File Entries
<code>#\$IMXE:< Keyword=value ></code>	<code>#\$IMXE: TYPE=server</code>
For example: <code>#\$IMXE: TYPE=server</code>	<code>16.26.176.92 EngProliant.compaq.com EngProliant #user comments</code>

To change the default globally so it affects the next file entry and all subsequent entries, use a statement as shown in the following example. The default is changed to router for the next entry. Router remains the default for all entries until another `#$IMXE_DEFAULT` statement changes the value. If a single instance of TYPE is changed by a `#$IMXE` statement, the default is not used for only the next entry and then reverts to router.

Keyword Statement	Hosts file entries
<code>#\$IMXE_DEFAULT: < Keyword=value></code>	<code>#\$IMXE_DEFAULT: TYPE=router</code>
For example: <code>#\$IMXE_DEFAULT: TYPE=router</code>	<code>16.26.176.92 BldRtr6.compaq.com BldRtr6 #user comments</code>

Note:



If a keyword parameter is omitted on a commented entry, the current default value is used. The current default is always the standard default unless a new default value was set using the `#$IMXE_DEFAULT` statement. For a keyword that contains more than one word, such as "management processor," enclose the full keyword in double quotation marks. Quotation marks are optional for single keywords like "server."

The following text quoted from a hosts file illustrates several statements. The explanations, which begin with the pound sign (#), are not displayed in the hosts file.

```
# Title: Systems in database
# Sorted by: IP address
# Date: 28-Mar-00 2:29:31 PM
# Author: administrator
```

The system EngProliant uses all current defaults. There are no additional comments.

```
16.26.176.92 EngProliant.compaq.com EngProliant #user comments
```

The system testServer in the following example defaults for TYPE. The defaults for SNMP Timeouts and Retries were restored for this system but only apply to testServer. The SNMP write community string default was changed and only applies to testServer.

```
#$IMXE: TYPE=Server
#$IMXE: SNMP_TIM=0 SNMP_RET=0 SNMP_MON=public
SNMP_CON=private
16.26.160.20 testServer.compaq.com testServer
```

All defaults in the following example for the system BldRtr1 are the same as for testServer, but had to be specified because they are not the global defaults. These changes apply only to BldRtr1.

```
#$IMXE: TYPE=Router
#$IMXE: SNMP_TIM=0 SNMP_RET=0 SNMP_MON=public
SNMP_CON=private
16.26.160.23 BldRtr1.compaq.com BldRtr1
```

For the system BldRtr5, the TYPE and protocols used for discovery were changed from the current defaults. Because the remaining keyword entries are missing, the standard defaults are applied for the SNMP timeouts, retries, and community strings.

```
#$IMXE: TYPE=Router
16.26.160.24 BldRtr5.compaq.com BldRtr5
```

For the system AcctServer, only the TYPE was changed from the current defaults.

```
#$IMXE: TYPE=Server
16.26.176.36 AcctServer.compaq.com AcctServer #user comments
```

The global default for TYPE was changed from Unknown to Router. All subsequent entries will be identified as routers until a TYPE statement is used to specify another type or restore the default.

```
#$IMXE_DEFAULT: TYPE=Router
```

```
16.25.176.38 FloorRtr2a.compaq.com FloorRtr2a #user comments
```

```
The default for the next host entry was changed to management
processor, which is enclosed in quotes. # $IMXE:
TYPE="Management Processor" AcctSvriLo.compaq.com
16.25.176.37 AcctSvriLo #user comments
```

...

Default Values

If a parameter is missing in the hosts file, the default is applied.

Keyword	Value	Description
TYPE	Application, Cluster, Complex, Desktop, Enclosure, Environmental Monitor, Handheld, Hub, KVM Switch, Management Processor, Notebook, Partition, Power Distribution Unit, Power Supply, Printer, Rack, Resource Partition, Remote Access Device, Router, Server, Shared Resource Domain, Storage Device, Switch, Tape Library, Thin Client, UPS, Unknown, Unmanaged, >Workstation Refer to "System Types" for more information on each system type.	Unknown (Default)
DMI	0	Disabled (Default)
	1	Enabled
SNMP	0	Disabled (Default)
	1	Enabled
HTTP	0	Disabled (Default)
	1	Enabled
SNMP_TIM	0	System default (Default)
	greater than 0	
SNMP_RET	0	System default (Default)
	greater than 0	

Keyword	Value	Description
SNMP_MON	Public <Community String >	Read only (Default)
SNMP_CON	<Community String>	No default

Related Procedure

- Managing Hosts Files

Related Topic

- Discovery and Identification

IP Ranges

You can specifically include or exclude IP addresses individually for discovery or as part of a range. IP address range entries also affect cluster discovery. The IP ranges must include the addresses of the cluster and its nodes. Enter one system or range per line. Use the following guidelines:

IP Range	Range to Enter
Your local subnet IP ranges from 1 to 254, the default Ping inclusion ranges	172.25.76.1-172.25.76.254
A single system as a range in the Ping inclusion ranges or Exclusion ranges fields	172.25.76.114-172.25.76.114 or 172.25.76.114
A group of systems within a subnet in the Ping inclusion ranges or Exclusion ranges fields	172.25.76.38-172.25.76.48
Systems included in a discovery template file	@DiscoveryTemplate_filename
Systems included in a hosts file	\$filename
No broadcast node in this subnet	172.25.76.255:NOBROADCAST
Broadcast node determined by the subnet mask	172.25.76.0-172.25.76.255:255.255.255.0 or 172.25.76.114:255.255.255.0

Discovery assumes you do not want to ping the subnet network ID, typically the zero node, or the subnet broadcast address, typically node 255, because these would unnecessarily take network resources. If the system 255 is not a broadcast address on your network, you can indicate this in the **Ping inclusion ranges** section as shown in the table or exclude the specific system in the **Exclusion ranges** section. HP Systems Insight Manager (HP SIM) uses the subnet mask to determine the broadcast system. If you do not specify a mask, HP SIM uses the default mask for the class of network. If your subnet mask is not the default for the class, the broadcast system can be included, generating much more network traffic than necessary.

Related Procedure

- Configuring Automatic Discovery

Related Topic

- Discovery and Identification

Identification

Identification follows automatic or manual discovery of a system and determines the following information about the discovered system:

- Management protocol the system uses (for example, Simple Network Management Protocol (SNMP), Desktop Management Interface (DMI), Web-Based Enterprise Management (WBEM), HTTP, Secure Shell (SSH)).
- Type of system (for example, server, client, management processor, storage, switch, router, or cluster)
- Product name of the system
- Operating system name, type, and version
- Associations, such as *iLO in server*

Note:



During identification, remote enclosures have a generic name (format: Encl_SerialNumber) assigned to them until one server from every enclosure is discovered and identified. Then the enclosures contain the name of the enclosure assigned to the enclosure.

For newly found automatically discovered systems, before the system is added to the database, any discovery filters that are configured are applied. If a system does not match the discovery filter, it is not added to the database, and no additional tasks or requests are made to that system. After the system passes the filter, it is added to the database. At this time, the system is available to any polling tasks, lists, or other operations.

Note:



Discovery filters do not apply to manually discovered systems.

HP Systems Insight Manager (HP SIM) performs initial hardware and software status polling and initial data collection on newly added systems. Refer to “Hardware Status Polling”, “Software Status Polling”, and “Data Collection” for more information on each task. The information about the systems is stored in the database.

The time to complete the discovery and identification cycle varies with the network size and resources. All necessary tasks are predefined in HP SIM. Predefined tasks cannot be removed from the system, but they can be disabled if needed. You can also create a new identification task and schedule it to run when you want to update identification information from systems.

By default, HP SIM runs System Identification once per day and when new systems are discovered. Most users do not need to schedule identification tasks to run more than once per day.

Initial Identification

After a system has been newly discovered or rediscovered, HP SIM attempts to identify it. The discovery task is not 100% complete until all the systems discovered or rediscovered have been identified.

Note:



If upgrading from Insight Manager 7 to HP SIM, you must run identification for all network devices, racks, and enclosures to be displayed on the **Status Overview** page.

Identify Systems

To identify systems in between discoveries, select **Options->Identify Systems**. The **Identify Systems** page appears. From this page, select target systems to add. Refer to “Creating a Task” for more information on selecting targets.

Related Procedure

- Adding a System Manually

Related Topic

- Discovery and Identification

Manage System Types

The System Type Manager (STM) is a utility to modify the default behavior of identification. STM enables you to customize the type and product name of systems using rules based on responses to SNMP and DMI (Windows only) lists from systems on your network.

Important:



For most HP systems, the system type and product name cannot be modified. Outside of this, identification can be customized based on SNMP System Object Identifiers (OIDs). Manufacturers assign unique system object identifiers to their SNMP instrumented products. STM enables you to customize identification by creating rules that map these system object identifiers to product categories and names of their choice. You must have full-configuration-rights to use STM.

To access the **Manage System Types** page, select **Options->Manage System Types**. From this page, you can:

- **Create a New Rule.** Click **New**.
- **Edit an Existing Rule.** Click **Edit**.

- **Delete an Existing Rule.** Click **Delete**. A confirmation box appears. Click **OK** to delete the rule, or click **Cancel** to cancel the deletion and return to the **Manage System Types** page.

Related Procedures

- Creating a New STM Rule
- Editing STM Rule
- Deleting STM Rule

Related Topics

- Navigating the Manage System Types Page
- Additional Information for Creating a New STM Rule
- About System Type Manager

Navigating the Manage System Types Page

The **Manage System Types** page lists rules currently defined in HP Systems Insight Manager (HP SIM). Refer to the following for more information on the page.

1. System Type
2. Columns
3. Total
4. Available Buttons

The screenshot shows the 'Manage System Types' interface. At the top, there's a navigation menu with options like Tools, Deploy, Configure, Diagnose, Optimize, Reports, Tasks & Logs, Options, and Help. Below that, the title 'Manage System Types' is displayed with a subtitle 'Create and manage rules to identify third party SNMP managed systems.' A dropdown menu for 'System type' is set to 'All'. A table of rules is shown with the following columns: Product Model, Product Type, Subtype, Protocol, Priority, and System Object Identifier. The table contains 10 rows of data. Below the table, there are three buttons: 'New...', 'Edit...', and 'Delete'.

Product Model	Product Type	Subtype	Protocol	Priority	System Object Identifier
3Com Hub 10	Hub	None	SNMP	1	1.3.6.1.4.1.43.1.8.5
3Com Hub 40	Hub	None	SNMP	1	1.3.6.1.4.1.43.1.8.27.4.1
3Com Linkswitch 1000	Hub	None	SNMP	1	1.3.6.1.4.1.43.1.8.13
AdvanceStack 12R with Management...	Switch	None	SNMP	1	1.3.6.1.4.1.11.2.3.7.5.15
AdvanceStack 16U with SNMP module	Switch	None	SNMP	1	1.3.6.1.4.1.11.2.3.7.5.12
AdvanceStack 24R with Management...	Switch	None	SNMP	1	1.3.6.1.4.1.11.2.3.7.5.16
AdvanceStack 24T with Management...	Switch	None	SNMP	1	1.3.6.1.4.1.11.2.3.7.5.17
AdvanceStack 8U with SNMP module	Switch	None	SNMP	1	1.3.6.1.4.1.11.2.3.7.5.11
AdvanceStack Switch 100	Switch	None	SNMP	1	1.3.6.1.4.1.11.2.3.7.5.9
AdvanceStack Switch 200	Switch	None	SNMP	1	1.3.6.1.4.1.11.2.3.7.5.10

To access the **Manage System Types** page, select **Options>Discovery>Manage System Types**.

System Type

The list can be filtered by system type by selecting a type from the **System Type** dropdown list. Click the down arrow, and select a system type by which to filter the list.

Columns

The following columns appear on the **Manage System Types** page:

- Product Model
- Product Type
- Sub Type
- Protocol
- Priority
- System Object Identifier

Click a column heading to sort the column in ascending or descending order.

Total

The **Total** displays the total number of systems that meet the System Type selected in the **System type** dropdown list.

Available Buttons

- **New**. Used to create a new rule.
- **Edit**. Used to edit existing rules. Select the rules to edit, and click **Edit**.
- **Delete**. Used to delete an existing SNMP or DMI rule. Select the rule, and click **Delete**. In the confirmation box, click **OK** to delete the rule, or **Cancel** to return to the **Manage System Types** page without deleting the rule.

Related Procedures

- Creating a New STM Rule
- Editing STM Rule
- Deleting STM Rule

Related Topics

- Manage System Types
- About System Type Manager

About System Type Manager

Manufacturers assign unique system object identifiers to their SNMP instrumented products. System Type Manager (STM) enables users to customize identification by creating rules that map these system object identifiers to product categories and names of their choice. HP Systems Insight Manager (HP SIM) discovers and applies information from the rule when an unknown system matches a rule that you specify. Rules contains system object identifiers, and optionally, additional object identifier, that are compared with responses from a target system. When a rule meets the comparison specification, the system is identified using information from the rule.

Note:



SNMP rules can be created from the **Manage System Types** page within HP SIM or from the CLI using the **mxstm** command. Additionally, on Windows systems, you can create rules based on the DMI protocol using the CLI **mxstm** command. Refer to the following procedures for more information on the CLI options.

Note:



SNMP rules require a system object identifier and product name. Optionally, a compare rule (match or starts with), MIB OID with value and compare rule, product type, subtype, custom management page, and priority can also be specified. DMI rules are specified by selecting a product name and at least one, or at the most three, DMI elements with response values and compare rules.

Why Add or Modify System Identification?

- You might have third-party systems on your network that are not included in the HP SIM database, and you want them identified by unique product names based on location or use.
- You have systems of a known type that you want to identify in another way. For example, you have laptops that you want to classify on some other basis.

Options for Creating a System Type Manager Rule

Systems are identified and classified using specific rules and are assigned a corresponding system type and a product name.

For SNMP systems, STM uses the System object identifier and optionally a MIB variable OID and its value and data type. Identification is based on the system object identifier returned from the system to be identified. If there is a matching rule for the system object identifier, identification proceeds based on whether the response value matches the criteria in the rule.

For DMI systems, STM uses requests consisting of one to three DMI elements. The elements are attribute and value pairs. For a rule to be applied, the returned response values must match values in the rule in a manner defined by the corresponding compare rules.

The custom management page is a link on the **System Page** under the **Tools & Links** tab. The link appears with other system links for the system if it is unique. You can specify a URL address that opens an HTML page. For example, enter:

`http://support.networkingcompany.com/model123` .

New system types are displayed in system collections after a full discovery runs and identifies systems that match rules you created.

You can modify and delete rules as the systems in your network change.

Related Procedures

- Creating a New STM Rule
- Editing STM Rule
- Deleting STM Rule

Related Topics

- Manage System Types
- Navigating the Manage System Types Page

Creating a New STM Rule

Perform this procedure to create a new SNMP rule through System Type Manager (STM).

The System Type Manager (STM) is a utility used to modify the default behavior of identification. STM enables you to customize the type and product name of systems using rules based on responses to SNMP and DMI (Windows only) collections from systems on your network.

Note:



DMI rules can only be created from the command line.

Note:



The following fields are required:

- System Object Identifier, including the Compare Rule
- System Type
- Product Name

To create a new SNMP rule:

1. Select **Options->Manage System Types**. The **Manage System Types** page appears.
2. Click **New**. The **New rule** section appears.
3. Enter the **System Object Identifier** information. Retrieve the system object identifier from a target system on your network by clicking **Retrieve from System**. The **Retrieve From System** section appears. This is a required field.

Retrieve from system:

Enter an object identifier, community string and target hostname or IP address and click on the 'Get response' button to view details below. Clicking 'OK' will transfer this value to the system object identifier field above.

- a. In the **Object Identifier** field, enter the object identifier.
- b. In the **Community String** field, enter the community string if other than the default, public. The community string of the target system and the HP Systems Insight Manager (HP SIM) server must match to retrieve data.
- c. In the **Target hostname or IP address** field, enter the IP address of the system you want to search.
- d. Click **Get Response** to show the **Response SNMP data type** and the **Response value**.
- e. Click **OK** to close the **Retrieve From System** section, and place the response value in the **System Object Identifier**, **Object Value** fields, or both.

4. Enter the **System Object Identifier Compare Rule**. Click the down arrow and select the appropriate rule. In most cases, this would be **match**. You can set it to **starts with** if you know that a class of systems has system object identifiers that start with the value you have entered.
5. (Optional) Specify **MIB variable object identifier** by clicking **Retrieve from MIB**. The **Retrieve from MIB** section appears.

You might need to do this if you have systems that return the same system object identifier that you would like to classify as different products based on some SNMP variable that returns a different value for each class. For example, if you have Windows NT servers from different vendors that return the same Windows NT system object identifier. You can specify rules using the Windows NT system object identifier as the system object identifier and a vendor-specific MIB variable and value combination to create separate rules for each vendor.

Retrieve from MIB:

Select a MIB file and MIB variable to view the MIB variable details below. Clicking 'OK' will transfer this value to the MIB Variable OID field above.

MIB definition file name:	rfc1213.mib
MIB variable name:	sysDescr
MIB variable object identifier:	1.3.6.1.2.1.1.1
MIB variable access:	READ-ONLY
MIB variable status:	MANDATORY
MIB variable type:	DISPLAYSTRING

- a. Click the down arrow in the **MIB definition file name** box to select the MIB definition file.
 - b. Click the down arrow in the **MIB variable name** box to select the MIB variable name.
 - c. Click **OK** to close the **Retrieve from MIB** section, and place the **MIB Variable Object Identifier** information in the field.
6. Select the **Object value** by clicking **Retrieve from system**. The **Retrieve from system** section appears.
 - a. Enter the **Object identifier**, **Community string**, and **Target hostname or IP address**.
 - b. Click **Get response** to view the **Response SNMP data type** and the **Response value**.
 - c. Click **OK** to close the **Retrieve from system** section, and place the information in the **Object value** field.
 7. Click the down arrow, and select the **Data Type** for the **Object value**.
 8. Click the down arrow, and select the **Compare Rule** for the **Object value**.
 9. Enter a **Priority** (applies only if there is more than one rule with the same system object identifier).
 10. In the **System Type** field, click the down arrow, and select the system type.
 11. In the **Subtype** field, click the down arrow, and select the system subtype.

12. In the **Product Name** field, enter the product name for the new rule.
13. In the **Custom management page** field, enter a URL. The URL displays this Web page as a system link on the **System Page** of systems identified using this rule. Enter the special keywords *\$ipaddress* and *\$hostname* anywhere in this URL. They are replaced by the actual IP address or hostname of the system when the link is placed on the **System Page**.
14. Click **Launch** to verify that you can browse to the URL.
15. Click **OK** to save the new rule, or click **Cancel** to cancel all changes and close the **New rule** section.

Command Line Interface

Use the **mxstm** command to add SNMP and DMI (Windows only) rules from the command line. For assistance with this command, refer to the HP-UX or Linux manpage by entering **man mxstm** at the command line. Refer to "Using Command Line Interface Commands" for more information on the command and how to access the manpage.

Related Procedures

- Editing STM Rule
- Deleting STM Rule

Related Topics

- Manage System Types
- About System Type Manager
- Navigating the Manage System Types Page

Editing STM Rule

Edit an existing SNMP rule using System Type Manager (STM) to change the priority, system type, subtype, or custom management page.

Note:



Changing the priority on this page reorders the priorities of all other rules with the same system object identifier such that all rules with the same system object identifier have a unique priority ranging from one to the number of rules with the same system object identifier.

Note:



All steps are optional.

To edit an SNMP rule:

1. Select **Options->Manage System Types**. The **Manage System Types** page appears.
2. Click **Edit**. The **Edit rule** section appears.
3. In the **Priority** field, change the priority.
4. In the **System Type** field, click the down arrow to change the system type.
5. In the **Subtype** field, click the down arrow to change the subtype.
6. In the **Custom management page** field, change the URL. Click **Launch** to verify that you can browse to the URL launch page.
7. Click **OK** to save changes and return to the **Manage System Types** page, or click **Cancel** to return to the **Manage System Types** page without saving any changes.

Related Procedures

- Creating a New STM Rule
- Deleting STM Rule

Related Topics

- Manage System Types
- About System Type Manager
- Navigating the Manage System Types Page

Deleting STM Rule

Perform the following procedure to delete a System Type Manager (STM).

To delete an STM rule:

1. Select **Options->Manage System Types**. The **Manage System Types** page appears.
2. Select the rule to delete.
3. Click **Delete**. A confirmation box is displayed.
4. Click **OK** to delete the rule, or click **Cancel** to cancel the deletion process.

Related Procedures

- Creating a New STM Rule
- Editing STM Rule

Related Topics

- Manage System Types
- About System Type Manager
- Navigating the Manage System Types Page

Additional Information for Creating a New STM Rule

Manufacturers assign unique system object identifiers to their SNMP instrumented products. In addition, systems supply information about themselves using variables described in files called Management Information Bases (MIBs). These values are enumerated using an industry-standard structure. MIBs are provided by vendors for their systems and must be registered with HP Systems Insight Manager (HP SIM) to be accessible and usable from System Type Manager (STM). HP preregisters all HP MIBs and many third-party MIBs. You can register the remaining MIBs using the MIB compiler, if you have the related systems on your network. Refer to “Registering a MIB” for information on registering MIBs. If you examine a MIB, you will find modules, or groups of variables. Some variables have multiple values. Each of these values has an object identifier as well. You can use these object identifiers to determine which system you have and their current behavior by querying these object identifiers.

Adding New DMI Rules (from Windows CMS Only)

You can create a new DMI-based rule using the command line utility (`mxstm`). DMI system information originates in Management Information Format (MIF) files. MIF files contain elements that have attributes and corresponding values. Refer to “Using Command Line Interface Commands” for information on accessing the `mxstm` manpage.

Adding New SNMP Rules

You can create a new SNMP-based rule using the command line utility (`mxstm`) or from the HP SIM user interface by selecting **Options->Manage System Types**. Within the SNMP framework, manageable network systems (routers, bridges, servers, and so on) contain a software component called a management agent. The agent monitors the various subsystems of the network element and stores this information in a MIB. The agents enable the system to generate traps, which can be configured to be sent to a trap destination server that is running HP SIM.

Things You Should Know About DMI Identification

DMI identification is based on how a system responds to a DMI request. Systems supply information about themselves as defined in files called MIFs. MIFs are vendor specific. Simply having a MIF file on a target system does not guarantee DMI identification. MIFs cannot be registered the way MIBs are registered in HP SIM. If you examine a MIF (for example, the generic `Win32s1.MIF`), you will find groups of attributes. The values returned in response to requests for MIF attributes can be used to determine which system you have and its current behavior.

For example, the following extract is part of the `Win32s1.MIF`. Notice the group named *Component ID*, followed by several attributes that identify one aspect of a DMI system, such as Manufacturer, Product, Version, and Serial Number. Other MIFs have different groups and specify other aspects of a system. The information in the MIFs is the information you supply to STM when you create a rule. STM can request a value from a specific target for a specific attribute.

Note:



DMI identification is only supported on Windows and HP-UX-based central management server (CMS) installs. In addition, only like operating systems can be

identified. For example, Windows-based CMSs can identify Windows-based DMI, and HP-UX-based CMSs can only identify HP-UX-based DMI systems.

```
Start Group
Name = "ComponentID"
ID = 1 Class = "DMTF|ComponentID|001"
Description = "This group defines the attributes common to
all components. This group is required."
```

```
Start Attribute
Name = "Manufacturer"
ID = 1 Description = "Manufacturer of this system."
Access = Read-Only
Storage = Common
Type = String(64)
Value = "Intel Corporation"
End Attribute
```

```
Start Attribute
Name = "Product"
ID = 2
Access = Read-Only
Storage = Common
Type = String(64)
Value = "Win32 DMI Service Layer"
End Attribute
```

```
Start Attribute
Name = "Version" ID = 3
Description = "Version number of this component."
Access = Read-Only
Storage = Common
Type = String(64)
Value = "2.32" End Attribute
```

```
Start Attribute
Name = "Serial Number" ID = 4 Access = Read-Only
Storage = Common Type = String(64)
Value = "unsupported"
End Attribute ...
```

Related Procedures

- Creating a New STM Rule
- Editing STM Rule
- Deleting STM Rule

Related Topics

- [Manage System Types](#)
- [About System Type Manager](#)
- [Navigating the Manage System Types Page](#)

Users and Authorizations

Note:



Users that have been added to the central management server (CMS) are unable to view or manage systems until authorizations have been configured for them.

Note:



HP-UX and Linux-provided command line tools, such as **ls** and **df**, are run as root by default. For security reasons, you might want them to run as a specific user to avoid permitting unintended capabilities to a user.

HP Systems Insight Manager (HP SIM) enables you to configure authorizations for specific users or user groups. Authorizations give the user access to view and manage systems. Each authorization specifies a user or user group, a toolbox, and a system or system group. The specific set of tools that can be run against a system is specified in the assigned toolbox.

It is important that you plan what systems each user is going to manage and which specific set of tools the users are authorized to execute against the managed systems. A user with no toolbox authorizations on a system cannot view or manage that system.

Authorizations are additive. If a user is authorized on Toolbox1 on a system, and is also authorized for Toolbox2 on the same system, the user is authorized for all tools in both Toolbox1 and Toolbox2 on that system. Similarly, a user authorized for the **All Tools** toolbox needs no other toolbox authorization on that system since the **All Tools** toolbox always includes all tools.

Refer to these general steps as a guideline for setting up user names and authorizations in the following sections:

1. "Configuring Automatic Discovery"
2. "Creating New Users"
3. "Creating New User Groups"
4. "Creating New Toolboxes"
5. "Creating New Authorizations"

User Configuration Rights

HP SIM provides the following configuration rights:

- **Full-configuration-rights.** Allows the user total control of the database. Users can run discovery of systems and data collection; define users and authorizations; set Cluster Monitor

configuration; configure licensing and protocol settings; and create, modify, delete, and run reports, snapshot comparisons, tools, custom commands, events, automation tasks, and so on.

- **Limited-configuration-rights.** Enables the user to create, edit, and delete reports (including predefined reports).
- **No configuration rights.** Enables the user to view and run predefined reports on systems they have been authorized to view only. A user with no configuration rights cannot execute any actions to affect the system database.

Users and Authorizations Tabs

The **Users and Authorizations** tabs offer the following options:

- **Add, edit, and delete users and user groups, and view and print user reports.** Select **Options->Security->Users and Authorizations->Users**.
- **Add, edit, and delete toolboxes, and view and print toolbox reports.** Select **Options->Security->Users and Authorizations->Toolboxes**.
- **Add and delete authorizations, and view and print authorization reports.** Select **Options->Security->Users and Authorizations->Authorizations**.

Related Procedures

- Creating New Users
- Creating New User Groups
- Creating New Toolboxes
- Creating New Authorizations
- Editing User Accounts and User Groups
- Editing Toolboxes
- Deleting User Accounts and User Groups
- Deleting Toolboxes
- Deleting Authorizations
- User and User Group Reports
- Toolbox Report
- Authorization Report

Related Topics

- Users and User Groups
- Toolboxes
- Authorizations

Users and User Groups

Administering users involves adding, editing, deleting, and reporting. After you have added a user or user group, you can assign predefined authorizations from the **Authorizations** tab.



Users and user groups must exist in the operating system. For Windows, this includes Active Directory. When a user group is configured in HP Systems Insight Manager (HP SIM), any user that is a member of the user group in the operating system can sign into HP SIM. This means they do not have to be configured as a user in HP SIM. The user can subsequently create tasks and run tools based on the user group's authorizations and configuration rights as configured in HP SIM.

The **Users** tab displays a table which includes the following information:

- **User/User Group.** This column includes all users and user groups. A user group is indicated by a bold font while group-based user accounts (member of a configured user group) are indicated by an italicized font.
- **Configuration Rights.** This column displays what type of configuration rights the user or user group has (full, limited, or none).
- **Pager Configuration.** This column displays if the user has a pager configured, and is blank for user groups.
- **IP Login Restrictions.** This column displays if there are any IP restrictions applied to the user or user group.
- **Full Name.** This column displays the full name for the user or group if this information was set during creation of the user or user group.

The **Users** tab provides the following options:

- **Create new users.** Select **Options>Security>Users and Authorizations>Users**, and then click **New**. The **New User** section appears.
- **Create new user groups.** Select **Options>Security>Users and Authorizations>Users**, and then click **New Group**. The **New User Group** section appears.
- **Edit existing users or user groups.** Select **Options>Security>Users and Authorizations>Users**, and select a user or user group. Click **Edit**. The **Edit User** or **Edit User Group** section appears. You can edit group-based (italicized) users to convert them to individually configured users.
- **Delete users or user groups.** Select **Options>Security>Users and Authorizations>Users**, and select users or user groups. Click **Delete**. A confirmation box appears. Click **OK** to delete the users or user groups, or click **Cancel** to cancel the deletion.
- **View and print user reports.** Select **Options>Security>Users and Authorizations>Users**, and then click **Report**. The **Users Report** pop-up window appears. If you would like to print the report, select **File>Print**.

Note:



To sort the information in ascending or descending order, click the appropriate column heading. The column heading that includes the arrow is the column by which the list is sorted. If the arrow is pointing up, the list is sorted in ascending order. If the arrow is pointing down, the list is sorted in descending order.

Related Procedures

- Creating New Users
- Creating New User Groups
- Editing User Accounts and User Groups
- Deleting User Accounts and User Groups
- User and User Group Reports

Related Topics

- Users and Authorizations
- Toolboxes
- Authorizations
- Default User Templates

Creating New Users

Create a new user account to sign into HP Systems Insight Manager (HP SIM). The account must be valid on the operating system (includes Active Directory on Windows) on the central management server (CMS), and will be authenticated by the CMS. You must know the operating system user account name of the user you are adding, but you do not need to know the password.

To create a new user:

1. Select **Options->Security->Users and Authorizations->Users**, and click **New**. The **New User** section appears.
2. In the **Login name (on central management server)** field, enter the operating system login account name to be used to sign into HP SIM. This field is required.

Note: The user cannot sign into HP SIM if the account is not a valid login. The account is not validated until the user tries to sign into HP SIM.

3. In the **Domain (Windows domain for login name)** field, enter the Windows domain name for the login name if the CMS is running a Windows operating system. If left blank, the system name of the CMS is used as the domain.
4. In the **Full name** field, enter the user's full name.
5. In the **Phone number** field, enter the user's phone number.
6. In the **E-mail address** field, enter the user's e-mail address.

7. In the **Copy all authorizations of this user or [template]** field, select a template or login that already has the predefined authorizations that you want to assign to the login account you are creating. Refer to “Default User Templates” for more information on default user templates.
8. In the **Central management server configuration rights** section, select the level of authority to assign to the new user from the following options:
 - **full, allowed to modify all central management server settings.** Allows the user total control of the database. Users can run discovery of systems and data collection define users and authorizations; set Cluster Monitor configuration; configure licensing and protocol settings; and create, modify, delete, and run reports, snapshot comparisons, tools, custom commands, events, automation tasks, and so on.
 - **limited, allowed to create/modify/delete all reports and their own tools.** Allows the user to create new reports, edit any reports, and delete any reports (including the predefined reports).
 - **none, no configuration of central management server allowed.** Allows the user to view and run predefined reports on the CMS and all managed systems. However, the user has no configuration rights on the CMS or on the managed systems.
9. Under the **Login IP Address Restrictions** section, in the **Inclusion ranges** field, enter the IP addresses of the systems that you want this user to be able to use as a client browsing into this CMS. If you list multiple IP addresses, separate them with a semicolon (;). Each range is a single IP address or two IP addresses separated by a dash (-). The IP addresses must be entered in the standard dotted form, for example, 15.1.54.133. Any spaces surrounding the semicolons or dashes are ignored. Spaces are not allowed within a single IP address in dotted form. Enter 0.0.0.0 to prevent a user from logging in through a remote system.

Important: If browsing from the central management server, ensure all IP addresses of the CMS are properly included. If browsing to **localhost** ensure the loopback address 127.0.0.1 is also included.
10. In the **Exclusion ranges** field, enter the IP address of the systems that should be excluded from this user as clients browsing into this CMS. Use the same format in the previous step for **Inclusion ranges**.

Note: Be sure to verify that your inclusion and exclusion ranges do not overlap.

Note: Steps 11 through 15 are only for a CMS running Windows.
11. Under the **Pager Information** section, in the **Phone number** field, enter the pager phone number of the user associated with this user account if you are using a Windows operating system. If the **Phone number** field is left blank, the paging information is not saved.
12. In the **PIN number** field, enter the PIN number associated with the pager phone number.
13. In the **Message length** field, select how many characters can be accepted in the paging message from the dropdown list.
14. In the **Baud rate** field, select the appropriate baud rate for the pager from the dropdown list.
15. In the **Data format** field, select the appropriate data format for the pager from the dropdown list.

16. Click **OK** to save and close the **New User** section. You can click **Apply** to save and keep the **New User** section open, or click **Cancel** to cancel the creation of this user.

The new user account is created.

Command Line Interface

Users with full-configuration-rights can use the **mxuser** command to create users from the command line interface (CLI)

Users with limited-configuration-rights can use the **mxexec** command to launch command tools on one or more systems from the CLI. For assistance with this command, refer to the associated manpage.

Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Editing User Accounts and User Groups
- Deleting User Accounts and User Groups
- User and User Group Reports

Related Topics

- Users and Authorizations
- Users and User Groups
- Default User Templates

Creating New User Groups

User groups must exist in the operating system. For Windows, this includes Active Directory. Members of the user groups in the operating system can sign into HP Systems Insight Manager (HP SIM) and will inherit the group's attributes for configuration rights and login IP address restrictions, as well as the group's authorizations. When a group's configuration rights, login IP address restrictions, or authorizations are changed, this change is immediately reflected in all current members of the group.

Users that are members of multiple user groups inherit attributes and authorizations from each group. For configuration rights, the user inherits the highest setting. For login IP address restrictions, the user inherits all entries. For authorizations, the user inherits all authorizations.

Note:



A user's group membership is determined at sign in. If a user's group membership changes in the operating system, it is not reflected in HP SIM until the next time the user signs in to HP SIM.

To create a new user group:

1. Select **Options->Security->Users and Authorizations->Users**, and click **New Group**. The **New User Group** section appears.

2. In the **Group name (on central management server)** field, enter the operating system group name to be used for logging into HP SIM. This field is required.
3. In the **Domain (Windows domain for login name)** field, enter the Windows domain name for the group if the central management server (CMS) is running a Windows operating system.
4. In the **Full name** field, enter the full name for the group. This is displayed in the table on the **Users** tab.
5. In **Copy all authorizations of this user or [template]** dropdown list, select a template or login that already has the predefined authorizations that you want to assign to the group you are creating. Refer to “Default User Templates” for more information on default user templates.
6. In the **Central management server configuration rights** section, select the level of authority to assign to the new user group from the following options. Users that login into HP SIM as members of this group inherit these configuration rights.
 - **full, allowed to modify all central management server settings.** Allows the user total control of the database. Users can run discovery of systems and data collection define users and authorizations; set Cluster Monitor configuration; configure licensing and protocol settings; and create, modify, delete, and run reports, snapshot comparisons, tools, custom commands, events, automation tasks, and so on.
 - **limited, allowed to create/modify/delete all reports and their own tools.** Allows the user to create new reports, edit any reports, and delete any reports (including the predefined reports).
 - **none, no configuration of central management server allowed.** Allows the user to view and run predefined reports on the CMS and all managed systems. However, the user has no configuration rights on the CMS or on the managed systems.
7. Under the **Login IP Address Restrictions** section, in the **Inclusion ranges** field, enter the IP addresses of the systems that you want members of this user group to be able to use as a client browsing into this CMS. If you list multiple IP addresses, separate them with a semicolon (;). Each range is a single IP address or two IP addresses separated by a dash (-). The IP addresses must be entered in the standard dotted form, for example, 15.1.54.133. Any spaces surrounding the semicolons or dashes are ignored. Spaces are not allowed within a single IP address in dotted form. Enter 0.0.0.0 to prevent a user from logging in through a remote system.

Important: If browsing from the central management server, ensure all IP addresses of the CMS are properly included. If browsing to **localhost** ensure the loopback address 127.0.0.1 is also included.
8. In the **Exclusion ranges** field, enter the IP address of the systems that should be excluded from members of this user groups as clients browsing into this CMS. Use the same format in the previous step for **Inclusion ranges**.

Note: Be sure to verify that your inclusion and exclusion ranges do not overlap.
9. Click **OK** to save and close the **New User Group** section. You can click **Apply** to save and keep the **New User Group** section open, or click **Cancel** to cancel to close the **New User Group** section without saving the new group.

Command Line Interface

Users with full-configuration-rights can use the **mxuser** command to create user group from the command line interface (CLI)

Users with limited-configuration-rights can use the **mxexec** command to launch command tools on one or more systems from the CLI. For assistance with this command, refer to the associated manpage.

Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Editing User Accounts and User Groups
- Deleting User Accounts and User Groups
- User and User Group Reports

Related Topics

- Users and Authorizations
- Users and User Groups
- Default User Templates

Editing User Accounts and User Groups

In the event a user account or user group must be modified, you can edit it from the **Users** tab on the **Users and Authorizations** page.

Note:



If a group's configuration rights or login IP address restrictions are changed, this is immediately reflected in all current members of the group. If a group name is edited, none of its current members are affected, other than to pick up the new group name.

Note:



A group-based user account can be edited only to convert to an individual user and is not reversible.

To edit a user account or user group:

1. Select **Options->Security->Users and Authorizations->Users**.
2. Select the user or user group you want to edit, and click **Edit**. The **Edit User** or **Edit User Group** section appears.
3. Change the appropriate setting.

Note: Steps d-e and i-m are not available for user groups.

- a. In the **Login name (on central management server)** field, edit the operating system name for the user or user group. This field is required.
- b. In the **Domain (Windows domain for login name)** field, edit the Windows domain name for the user or user group name if the central management server (CMS) is running Windows.

Note: If the user account was migrated from Insight Manager 7, the **Domain (Windows® domain for login name)** field has a dummy domain associated with the user. If the user is a user that receives pages, this field must be edited to include a valid domain on your network.

- c. In the **Full name** field, edit the full name for the user or group. This does not apply to user groups.
- d. In the **Phone number** field, edit the user's phone number. This does not apply to user groups.
- e. In the **E-mail address** field, edit the user's e-mail address.
- f. In the **Central management server configuration rights** section, select the level of authority to assign to the user or user group from the following options:

- **full, allowed to modify all CMS settings.** Enables the user total control of the database. Users can run discovery of systems and data collection; define users and authorizations; set Cluster Monitor configuration; configure licensing and protocol settings; and create, modify, delete, and run reports, snapshot comparisons, tools, custom commands, events, automation tasks, and so on.
- **limited, allowed to create/modify/delete all reports and their own tools.** Enables the user to create new reports, edit any reports, and delete any reports (including the predefined reports).
- **none, no configuration of CMS allowed.** Allows the user to view and run predefined reports on the CMS and all managed systems. However, the user has no configuration rights on the CMS or on the managed systems.

CAUTION: If a user has been changed from a full-configuration-rights user, you might want to change the user's authorizations. Otherwise, the user might still have undesired tool authorizations, such as **All Tools** toolbox on **All Managed Systems** or **All Tools** toolbox on the CMS.

Refer to "Creating New Users" for more detailed information on each level of authority.

- g. Under the **Login IP Address Restrictions** section, in the **Inclusion ranges** field, edit the IP addresses of the systems that you want included for management by this user or user group. If you list multiple IP addresses, separate them with a semicolon (;). Each range is a single IP address or two IP addresses separated by a dash (-). The IP addresses must be entered in the standard dotted form, for example, 15.1.54.133. Any spaces surrounding the semicolons or dashes are ignored. Spaces are not allowed within a single IP address in dotted form.

Important: If browsing from the central management server, ensure all IP addresses of the CMS are properly included. If browsing to **localhost** ensure the loopback address 127.0.0.1 is also included.

- h. In the **Exclusion ranges** field, edit the IP address of the systems that should be excluded from management by this user or user group. Use the same format in the previous step for **Inclusion ranges**. Enter 0.0.0.0 to prevent a user from logging in through a remote system.

Note: Be sure to verify that your inclusion and exclusion ranges do not overlap.

Note: The following five steps are for Windows systems only and not for user groups.

- i. Under the **Pager Information** section, in the **Phone number** field, edit the pager phone number of the user associated with this user account if you are using a Windows operating system. If the **Phone number** field is left blank, the paging information is not saved.
 - j. In the **PIN number** field, edit the PIN number associated with the pager phone number.
 - k. In the **Message length** field, select how many characters can be accepted in the paging message from the dropdown list.
 - l. In the **Baud rate** field, select the appropriate baud rate for the pager from the dropdown list.
 - m. In the **Data format** field, select the appropriate data format for the pager from the dropdown list.
4. Click **OK** to save and close the **New User** section. You can click **Apply** to save and keep the **Edit User** section open, or click **Cancel** to cancel the modifications.

The user or group changes are saved.

Command Line Interface

Users with full-configuration-rights can use the **mxuser** command to modify users or user groups from the command line interface (CLI).

Users with limited-configuration-rights can use the **mxexec** command to launch command tools on one or more systems from the CLI. For assistance with this command, refer to the associated manpage.

Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Users and Authorizations
- Creating New Users
- Creating New User Groups
- Deleting User Accounts and User Groups
- User and User Group Reports

Related Topics

- Users and Authorizations
- Users and User Groups

Deleting User Accounts and User Groups

If an HP Systems Insight Manager (HP SIM) user account or user group is deleted from the operating system or has been disabled or locked out and the user account is already signed into HP SIM, the signed in user is not affected. Therefore, to remove a signed in user from HP SIM, the user account must be deleted from within HP SIM. This forces the user account to log out if it is already signed into HP SIM.

When deleting a user group, all members of the group lose membership in that group. This causes those users' authorizations, configuration rights, and login IP address restrictions to be updated based on their new group memberships. For users that are no longer members of any user group, they are deleted from HP SIM.

Caution:



Deleting a user or user group deletes the ability to log in as well as all associated authorizations and tasks owned by the affected user.

Note:



You cannot remove the last user account with full-configuration-rights.

To delete a user account or user group:

1. Select **Options->Security->Users and Authorizations->Users**.
2. Select the users and groups to be deleted.
3. Click **Delete**.
4. A confirmation box appears. Click **OK** to delete the selected users and user groups, or click **Cancel** to cancel the deletion process and return to the **Users** section. If deleting a user group also deletes any members of the group, a second confirmation box appears listing which users will be deleted. Click **OK** to continue and delete all listed users, or click **Cancel** to cancel the deletion process and return to the **Users** section.

The users, user groups, associated authorizations, and tasks are permanently deleted.

Command Line Interface

Users with full-configuration-rights can use the **mxuser** command to modify users and user groups from the command line interface (CLI).

Users with limited-configuration-rights can use the **mxexec** command to launch command tools on one or more systems from the CLI. For assistance with this command, refer to the associated manpage.

Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Creating New Users
- Creating New User Groups
- Editing User Accounts and User Groups
- User and User Group Reports

Related Topics

- Users and Authorizations
- Users and User Groups

User and User Group Reports

For detailed information regarding users and user groups, you can generate and print a report.

Note:



To sort the information in ascending or descending order, click the appropriate column heading. The column heading that includes the arrow is the column by which the report is sorted. If the arrow is pointing up, the report is sorted in ascending order. If the arrow is pointing down, the report is sorted in descending order.

The following summary information regarding all users appears in the **Users Report** window, along with the date and time of the report:

- **User/User Group**
- **Configuration Rights**
- **Pager Configured**
- **IP Login Restrictions**
- **Full Name**

To generate and print a user account or user group report:

1. Select **Options->Security->Users and Authorizations->Users**.
2. Click **Report**.

The **Users Report** window appears.

3. Select **File->Print** to print the report.

The user report is printed.

Command Line Interface

Users with full-configuration-rights can use the **mxuser** command to create user and user group reports from the command line interface (CLI).

Users with limited-configuration-rights can use the **mxexec** command to launch command tools on one or more systems from the CLI. For assistance with this command, refer to the associated manpage.

Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Creating New Users
- Creating New User Groups
- Editing User Accounts and User Groups
- Deleting User Accounts and User Groups

Related Topics

- Users and Authorizations
- Users and User Groups

Default User Templates

The default templates have predefined authorizations that are assigned to the new login account you are creating. This authorization gives the user access to systems and creates the relationship between toolboxes and discovered systems. Separate tools are provided for each access level, and the user can be authorized for these user-access tools in the **Monitor Tools** toolbox, while administrative-access tools are assigned in the **All Tools** toolbox.

There are three default user templates available in HP Systems Insight Manager (HP SIM). They are:

- **Administrator-template.** This template automatically gives the user full-configuration-rights on the central management server (CMS) and includes the **All Tools** toolbox for the CMS and for **All Managed Systems** as well.
- **Operator-template.** This template gives the user limited-configuration-rights on the CMS and includes authorizations for the **Monitor Tools** toolbox on the CMS and includes the **All Tools** toolbox on **All Managed Systems**.
- **User-template.** This template gives the user no configuration rights on the CMS and includes authorizations for the **Monitor Tools** toolbox for the CMS and **All Managed Systems**.

Related Topics

- Creating New Users

- Creating New User Groups
- Toolboxes

Toolboxes

The **Toolboxes** section enables you to configure groups of tools. The All Tools toolbox and the Monitor Tools toolbox are created during the installation process.

- The **All Tools** toolbox contains all tools in the central management server (CMS).
- The **Monitor Tools** toolbox contains tools that display the state of the managed systems, but not tools that change the state of the managed systems. For example, the **Monitor Tools** toolbox permits viewing installed software but not installing software.
- When HP Storage Essentials is installed, a Toolbox for Storage Essentials tools is added to this page. Refer to your HP Storage Essentials documentation for more information.

The **Toolboxes** tab provides the following options:

- **Create new toolboxes.** Select **Options>Security>Users and Authorizations>Toolboxes**, and then click **New**. The **New Toolbox** section appears.
- **Edit existing toolbox.** Select a toolbox to edit, and then select **Options>Security>Users and Authorizations>Toolboxes**. Then click **Edit**. The **Edit Toolbox** section appears.
- **Delete toolboxes.** Select toolboxes to delete. Select **Options>Security>Users and Authorizations>Toolboxes**. A confirmation box appears. Click **OK** to delete the toolboxes, or click **Cancel** to cancel the deletion.
- **View and print toolbox reports.** Select **Options>Security>Users and Authorizations>Toolboxes**, then click **Report**. The **Toolboxes Report** appears. Select **File>Print** to print the report.

Note:



To sort the information in ascending or descending order, click the appropriate column heading. The column heading that includes the arrow is the column by which the list is sorted. If the arrow is pointing up, the list is sorted in ascending order. If the arrow is pointing down, the list is sorted in descending order.

Related Procedures

- Creating New Toolboxes
- Editing Toolboxes
- Deleting Toolboxes
- Toolbox Report

Related Topics

- Users and User Groups

- Authorizations
- Default User Templates

Creating New Toolboxes

Create a toolbox to configure a group of tools to which a user has access.

Note:



The toolbox name must start with an alphabetic character followed by alphanumeric characters, embedded blank characters, underscore (_), or dash (-) and must be less than or equal to 16 characters in length.

To add a toolbox:

1. Select **Options->Security->Users and Authorizations->Toolboxes**, and then click **New**. The **New Toolbox** section appears.
2. In the **Name** field, enter a name for the new toolbox. This field is required.
3. In the **Description** field, enter a description for the toolbox.
4. Select **Toolbox is enabled** to enable the toolbox and all authorizations created with this toolbox.
5. In the **Show tools in category** field, select the category to display a list of tools in the available tools list. Select the tools to be assigned to this toolbox in the available tools list, and click **>>**.

The selected tools appear in the **Toolbox contents** list. You can select a tool displayed in the **Toolbox contents** list, and click **<<** to remove it from the assigned tools list.

6. Click **OK** to save the new toolbox and close the **New Toolbox** section. Click **Apply** to save the settings without closing the **New Toolbox** section, or click **Cancel** to cancel the new toolbox creation and return to the **Toolboxes** section.

Command Line Interface

Users with full-configuration-rights can use the **mxtoolbox** command to add toolboxes from the command line interface (CLI).

Users with full-configuration-rights can use the **mxexec** command to launch command tools on one or more systems from the CLI. For assistance with this command, refer to the associated manpage.

Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Editing Toolboxes
- Deleting Toolboxes
- Toolbox Report

Related Topics

- Users and Authorizations
- Toolboxes

Editing Toolboxes

You can change toolboxes to modify the contents of the toolbox, as well as its name and description.

Note:



The All Tools toolbox cannot be edited. However, the Monitor Tools toolbox can be edited, but only the set of tools that are contained in the toolbox can be changed.

To modify a toolbox:

1. Select **Options->Security->Users and Authorizations->Toolboxes**.
2. Select the toolbox to edit, and click **Edit**. The **Edit Toolbox** section appears.
3. Change the appropriate setting. Refer to “Creating New Toolboxes” for more detailed information on each field.

Note:



New custom command tools are located under **Tools->Custom Commands->Application Launch Tools**.

4. Click **OK** to save the changes, or click **Cancel** to cancel the changes.

Command Line Interface

Users with full-configuration-rights can use the `mxtoolbox` command to modify toolboxes from the command line interface (CLI).

Users with limited-configuration-rights can use the `mxexec` command to launch command tools on one or more systems from the CLI. For assistance with this command, refer to the associated manpage.

Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Creating New Toolboxes
- Deleting Toolboxes
- Toolbox Report

Related Topics

- Users and Authorizations
- Toolboxes

Deleting Toolboxes

Caution:



When a toolbox is deleted, all of the associated authorizations are also deleted.

Note:



The All Tools toolbox and the Monitor Tools toolbox cannot be deleted.

To delete a toolbox:

1. Select **Options->Security->Users and Authorizations->Toolboxes**.
2. Select the toolboxes to be deleted.
3. Click **Delete**. A confirmation box appears.
4. Click **OK** to delete the toolboxes, or click **Cancel** to cancel the deletion process.

The toolbox and all associated authorizations are permanently deleted.

Command Line Interface

Users with full-configuration-rights can use the `mxtoolbox` command to delete toolboxes from the command line interface (CLI).

Users with limited-configuration-rights can use the `mxexec` command to launch command tools on one or more systems from the CLI. For assistance with this command, refer to the associated manpage.

Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Creating New Toolboxes
- Editing Toolboxes
- Toolbox Report

Related Topics

- Users and Authorizations
- Toolboxes

Toolbox Report

For detailed information regarding a toolbox, you can generate and print a toolbox report.

Note:



To sort the report information in ascending or descending order, click the appropriate column heading. The column heading that includes the arrow is the column by which the report is sorted. If the arrow is pointing up, the report is sorted in ascending order. If the arrow is pointing down, the report is sorted in descending order.

The following information regarding all toolboxes appears in the **Toolboxes Report** window, along with the date and time of the report:

- **Toolbox**
- **Enabled**
- **Tools**
- **Description**

To print a toolbox report:

1. Select **Options->Security->Users and Authorizations->Toolboxes**.
2. Click **Report**.

The **Toolboxes Report** window appears.

3. Select **File->Print** to print the report.

The toolbox report is printed.

Command Line Interface

Users with full-configuration-rights can use the **mxtoolbox** command to generate and run reports from the command line interface (CLI).

Users with limited-configuration-rights can use the **mxexec** command to launch command tools on one or more systems from the CLI. For assistance with this command, refer to the associated manpage.

Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Creating New Toolboxes
- Editing Toolboxes
- Deleting Toolboxes

Related Topics

- Users and Authorizations
- Toolboxes

Authorizations

Authorizations give the user access to view and manage systems. An authorization is composed of users, toolboxes, and discovered systems. When you first access the **Authorizations** tab, a table is displayed listing all authorizations and includes the following information:

- **User/User Group.** This column includes all valid users and user groups. A user group is indicated by a bold font. Group-based users are not displayed in this table. However, they are listed in the **authorizations for users** table and are indicated by an italicized font.
- **Toolbox.** This column displays the toolboxes assigned to the user or user group for each authorization.
- **System.** This column displays the systems on which the user or user group has authorizations. A system group is indicated by a bold font.

	User/User Group	Toolbox	Systems
<input type="checkbox"/>	VVO-SIMAdmins	All Tools	CMS
<input type="checkbox"/>	<i>VVO-SIMAdmins</i>	All Tools	All Managed Systems
<input type="checkbox"/>	VVOAdministrator	All Tools	CMS
<input type="checkbox"/>	<i>VVOAdministrator</i>	All Tools	All Managed Systems
<input type="checkbox"/>	VVO-GM User	Monitor Tools	All Servers 001

A system group is a group of systems based on a system collection and used for authorizations. It is a static snapshot of the contents of the collection at the time the system group was created. If you click a system group name in the **Systems** column, a window appears showing systems that are currently contained in the system group. Click **OK** to close the window. To update the contents of the system group based on its source collection, you must update the authorization.

You can view all authorizations, or you can view filtered authorizations for users, user groups, toolboxes, system groups, and individual systems. Select the option from the **Authorizations for** box. Next select the name from the **Select name** box.

The **Authorizations** tab provides the following options:

- **Creating new authorizations.** Select **Options->Security->Users and Authorizations->Authorizations**, and then click **New**. The **New Authorizations** section appears. This option is not available for group-based users. Instead, create authorizations for the group-based user's user groups.
- **Deleting authorizations.** Select **Options->Security->Users and Authorizations->Authorizations**, select authorizations to delete and click **Delete**. A dialog box appears. Click **OK** to delete the authorizations, or click **Cancel** to cancel the deletion. This option is not available for group-based users. Instead, delete authorizations for the group-based user's user groups.
- **Viewing and printing authorization reports.** Select **Options->Security->Users and Authorizations->Authorizations**, and then click **Report**. The **Authorizations Report** pop-up window appears. To print the report, select **File->Print**.
- **Updating authorizations.** Select **Options->Security->Users and Authorizations->Authorizations**, and select an authorization using a system group based on a collection, and then click **Update**. The **Update Authorizations** section appears.

Note:



To sort the information in ascending or descending order, click the appropriate column heading. The column heading that includes the arrow is the column by which the list is sorted. If the arrow is pointing up, the list is sorted in ascending order. If the arrow is pointing down, the list is sorted in descending order.

Related Procedures

- Creating New Authorizations
- Deleting Authorizations
- Updating Authorizations
- Authorization Report

Related Topics

- Users and Authorizations
- Users and User Groups
- Toolboxes
- Default User Templates

Creating New Authorizations

Note:



To create authorizations with individual systems, be sure the systems have been discovered and are accessible in the database.

Note:

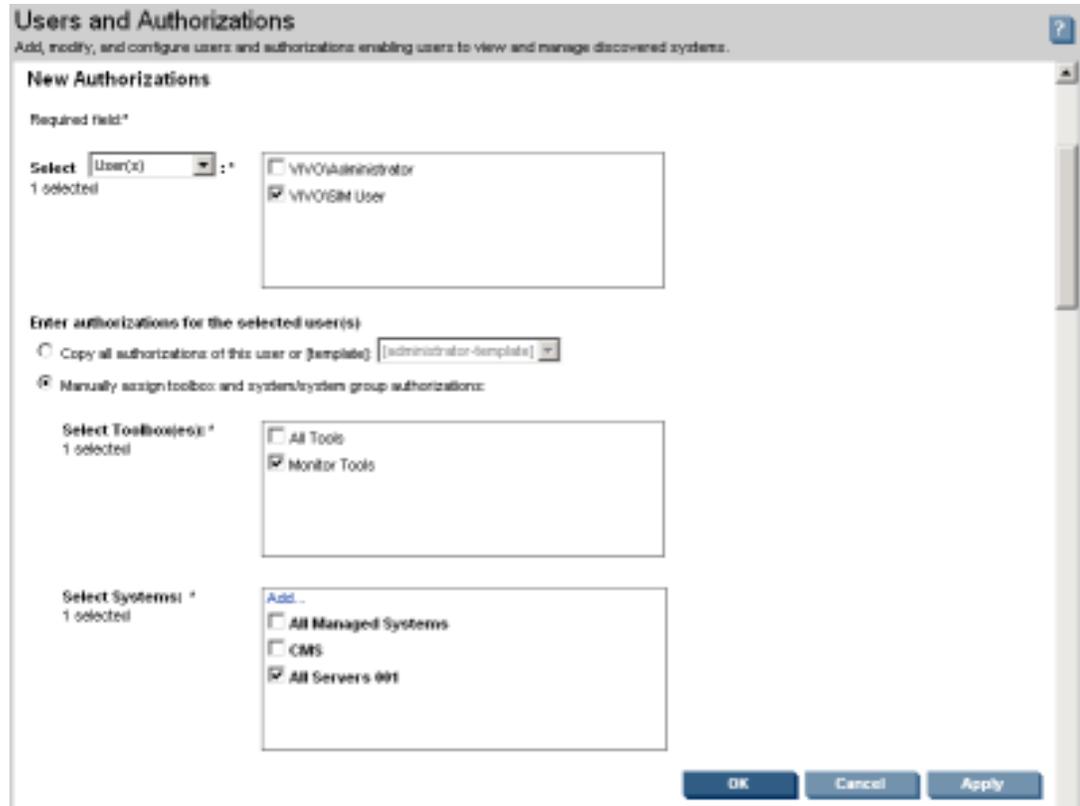


You cannot directly create new authorizations for group-based users.

To add a new authorization:

1. Select **Options->Security->Users and Authorizations->Authorizations**, and then click **New**. The **New Authorizations** section appears.
2. In the **Select** dropdown list, select **User(s)** or **UserGroup(s)**, and select the users or groups in the box. This field is required.
3. In the **Enter authorizations for the selected user(s)** section, select one of the following options:
 - **Copy all authorizations of this user or [template]:**

Select a user or template from the dropdown list.
 - **Manually assign toolbox and system/system group authorizations**
 - a. In the **Select Toolbox(es)** section, select the toolboxes to include.
 - b. In the **Select Systems** list box, the two default system groups are displayed. Select one of these groups or click **Add** to display the **Add Systems** section to select systems for the authorization.
 1. Click the down arrow in the **Add targets by selecting from** dropdown list and select a collection.
 2. If you want to use the entire collection as your selection, select **Select "collection name" itself**; this creates a system group based on the currently displayed contents of the collection.



3. If you want to select all individual systems from the collection, select the checkbox at the top of the table view to select all systems.

Note: This creates a separate authorization for each selected system.

4. If you want to select individual systems from the collection, select the systems from the table view.

Note: This creates a separate authorization for each selected system.

5. Click **Apply** to save system selections and return to the **New Authorizations** section, or click **Cancel** to return to the **New Authorizations** section without saving changes.

Note: A system group is a group of systems based on a system collection and used for authorizations. It is a static snapshot of the contents of the collection at the time the system group was created. There are two default system groups that are not based on collections. The **All Managed Systems** system group contains every managed system, except the central management server (CMS). The CMS is excluded so that users are not mistakenly assigned the authorization to manage the CMS system itself. There is a CMS group created explicitly for the CMS. These default system groups cannot be edited, updated, or deleted.

- c. If you selected individual systems of a collection, each selection populates the list box and is selected for inclusion in the authorization. If you selected a collection and the collection has been used previously in an authorization, a message appears stating that a system group for the collection exists and will be updated with current source collection content. This affects all authorizations associated with that collection. When

a collection is used for the first time, no message appears. A system group with the name of the collection followed by three numbers, usually 001, is displayed in the **Select Systems** dropdown list and is selected.

- d. Click **OK** to save the new authorization and close the **New Authorizations** section, or if you do not want to save changes, click **Cancel** to cancel the creating process.

Note:



When upgrading to HP Systems Insight Manager (HP SIM) 5.0 from any other version of HP SIM, any system groups the user created are migrated, but now become top-level collections. To manage system groups you now use the feature to edit a collection and update an authorization. Refer to “Editing System or Cluster Collections” and “Updating Authorizations” for more detailed information.

Command Line Interface

Users with full-configuration-rights can use **mxngroup** to create and manage system groups from the command line interface (CLI)

Users with full-configuration-rights can use the **mxauth** command to add authorizations from the CLI.

Users with full-configuration-rights can use the **mxexec** command to launch command tools on systems from the CLI. For assistance with this command, refer to the associated manpage.

Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Deleting Authorizations
- Authorization Report
- Updating Authorizations

Related Topics

- Users and Authorizations
- Authorizations

Updating Authorizations

This option is only available for authorizations using system groups based on a collection. It allows the contents of a system group to be updated to the current contents of its source collection. All authorizations using this system group (collection) are updated.

To update an authorization:

1. Select **Options->Security->Users and Authorizations->Authorizations**, select an authorization based on a system group, and then click **Update**. The **Update Authorizations** section appears.

2. In the **Show** dropdown list, select **changes**, **current contents**, or **updated contents**.
 - **changes.** Describes the specific changes that occur to the system group if updated. **Systems to Add** shows new systems that will be added to the system group and for all authorizations based on the system group. **Systems to Remove** shows current systems that will be removed from the system and from all authorizations using the system group. **Systems Unchanged** shows a list of systems that are unaffected by the update; they remain unchanged in the system group and all authorizations based on the system group.



- **current contents.** Shows the current contents of the system group.
 - **updated contents.** Shows what the contents of the system group will be after updating. This applies to authorizations based on this system group.
3. Click **Update Contents** to update the authorization, or click **Cancel** to cancel the update.

Command Line Interface

Users with full-configuration-rights can use `mxnngroup` to update system groups from the command line interface (CLI). However, if there are edits to the system group from the CLI, there is no affect on the source collection.

Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Creating New Authorizations
- Deleting Authorizations
- Authorization Report

Related Topics

- Users and Authorizations
- Authorizations

Deleting Authorizations

Caution:



If all authorizations are deleted, no one, not even a user with full-configuration-rights, can view or manage any systems.

To delete an authorization:

1. Select **Options->Security->Users and Authorizations->Authorizations**.
2. Select the authorizations to be deleted.
3. Click **Delete**. A confirmation box appears.
4. Click **OK** to delete the authorizations, or click **Cancel** to cancel the deletion process and return to the **Authorizations** section.

Authorizations cannot be directly deleted for group-based users. Instead, delete the authorizations for the group-based user's user group.

Note:



When deleting the last authorization using a system group, other than the default **All Managed Systems** of **CMS** system groups, the system group is also deleted.

Command Line Interface

Users with full-configuration-rights can use the **mxngroup** command to delete system groups from the command line interface (CLI).

Users with full-configuration-rights can use the **mxauth** command to delete authorizations from the command line interface (CLI).

Users with limited-configuration-rights can use the **mxexec** command to launch command tools on one or more systems from the CLI. For assistance with this command, refer to the associated manpage.

Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Creating New Authorizations
- Authorization Report
- Updating Authorizations

Related Topics

- Users and Authorizations
- Authorizations

Authorization Report

Generate an **Authorizations Report** to view and print authorizations. The **Authorizations Report** is tailored to the current filtered view. For example, if **user** is selected in the **Authorizations for** box, a report is generated for only the user selected. If **(none)** is selected in the **Select name** dropdown list, a report is generated for all of what is selected in the **Authorizations** box.

Note:



To sort the report information in ascending or descending order, click the appropriate column heading. The column heading that includes the arrow is the column by which the report is sorted. If the arrow is pointing up, the report is sorted in ascending order. If the arrow is pointing down, the report is sorted in descending order.

The following information regarding authorizations appears in the **Authorizations Report** window along with the date and time of the report:

- **User/User Group**
- **Toolbox**
- **System**

To view and print authorizations report:

1. Select **Options->Security->Users and Authorizations->Authorizations**.
2. Select an authorization from the **Authorizations for** dropdown list.
3. (Optional) Select a name from the **Select name** dropdown list.
4. Click **Report**.

The **Authorizations Report** appears.

5. Select **File->Print** to print the report.

The **Authorizations Report** is printed.

Command Line Interface

Users with full-configuration-rights can use the **mxngroup** command to generate and run system group reports from the command line interface (CLI).

Users with full-configuration-rights can use the **mxauth** command to generate and run reports from the CLI.

Users with limited-configuration-rights can use the **mxexec** command to launch command tools on one or more systems from the CLI. For assistance with this command, refer to the associated manpage.

Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Creating New Authorizations
- Deleting Authorizations
- Updating Authorizations

Related Topics

- Users and Authorizations
- Authorizations

System Groups

A system group is a group of systems used solely for authorizations. System groups can be managed directly from the command line interface (CLI) using the **mxngroup** command, or they can be managed indirectly through the GUI.

Managing System Groups from the GUI

A system group is created when an authorization is created using a system collection. This system group is named after the collection with three digits appended, usually 001. For example, All Racks 001. The system group contains the systems that were displayed during system selection, and is saved when the authorization is created.

Note:



Any further changes to the system collection do not affect the system group or authorizations, unless updated by one of the following options.

The contents of the system group is updated with the current contents of the collection when:

- Another authorization is created using the collection
- An authorization using the system group is updated
- Using **mxngroup** from the CLI

In the first two cases, the current contents of the collection are displayed for verification.

When deleting authorizations, a system group that is no longer used in any authorization is deleted.

Managing System Groups from the CLI Using Mxngroup

System groups can be created directly using the `mxngroup` command. When system groups are created in this manner, a top-level collection is created and named after the system collection with three digits appended, usually 001. The collection contains the systems in the system group only when the system group is first added, later modifications will not be reflected in the collection.

Note:



Additional changes to the system group or the collection do not affect the other, unless updated by one of the following options or by using the GUI as described above. Therefore, changes to the collection do not affect authorizations, and changes to the system group do not affect the collection view unless specifically updated.

The contents of the system group can be updated with the current contents of the collection by using the `-u` parameter for `mxngroup`:

```
mxngroup -m -g <groupname> -u
```

Caution:



This does not display the systems in the collection. To display the updated contents of the system group, use `mxngroup -lm -g <groupname>`.

Caution:



Setting up a periodic task to dynamically update a system group is not recommended. A collection based on system attribute scan can be compromised, adversely affecting authorizations in HP Systems Insight Manager (HP SIM), if those attributes are based on a non-secure protocol such as SNMP, or are maintained by a user with no configuration rights. Additionally the collection itself can be modified by a user with no configuration rights, again adversely affecting authorizations.

When deleting authorizations, a system group that is no longer used in any authorizations is deleted.

Related Procedures

- Creating New Authorizations
- Updating Authorizations

Related Topic

- Users and Authorizations

Networking and Security

HP Systems Insight Manager (HP SIM) provides the following security options:

- **User and Authorizations.** Select **Options>Security>Users and Authorizations.**
- **Server Certificate.** Select **Options>Security>Certificates>Server Certificate.**
- **Trusted Certificate.** Select **Options>Security>Certificates>Trusted Certificate.**
- **Login Event Settings.** Select **Options>Security>Login Event Settings.**
- **System Link Configuration.** Select **Options>Security>System Link Configuration.**

Secure Sockets Layer and Certificates

Secure Sockets Layer (SSL) is used between the browser and HP SIM to ensure data integrity and privacy. An integral part of SSL is a certificate, which is a public document used to identify the HP SIM server. When HP SIM is installed, it creates a self-signed certificate. Your browser might initially display a security alert when you browse to HP SIM, describing the certificate as untrusted. This designation occurs because the certificate is self-signed (signed by the HP SIM server) and the signer is not in the browser's list of Certification Authorities. By securely importing the HP SIM server certificate into the browser, the browser can authenticate the HP SIM server to which you are browsing. Refer to "Server Certificates" for more information about importing certificates into your browser.

HP SIM also supports the ability to use a certificate from a third-party Certificate Authority (CA) or your own internal CA or Public Key Infrastructure (PKI). In this case, you can import the CA certificate into your browser. Refer to "Importing a CA-Signed Certificate" for more information.

Login and Accounts

A user name, domain name (for Windows CMS), and password are required before accessing any feature of HP SIM. HP SIM uses the user authorizations of the underlying operating system (Windows, Linux, or HP-UX) and relies on the operating system to authenticate users.

The user installing HP SIM must be an administrator of the system (for Windows) or root (for Linux and HP-UX). This user is given administrative access to HP SIM.

After logging in with this account, create additional accounts for other users. Each account can be set up with different configuration rights and authorizations. You can also restrict the IP addresses from which each account can log in. Refer to "Users and Authorizations" for more information.

Audit settings can also be configured to log a notice for different types of login and logout events. Refer to "Configuring Login Events" for more information.

Single Login, Replicate Agent Settings, and Install Software and Firmware

To take advantage of single login or to execute Replicate Agent Settings or Install Software and Firmware tasks against managed systems, set up a trust relationship between HP SIM and the desired managed systems. A trust relationship allows the managed system to specify which HP SIM servers can issue commands to the system. Without an established trust relationship, these commands fail.

Setting up a trust relationship at the managed system involves browsing to the system, setting the trust mode, and adding HP SIM to the Trusted System Certificates list. Managed systems can also be set up with an appropriate certificate during deployment. Refer to “Initial ProLiant Support Pack Install” for more information. At the HP SIM server, you must also specify users' authorization for the managed system and have executed a System Identification Task. If you have enabled the **Require trusted certificates** option on the **Trusted System Certificates** page, you must import the certificates of trusted managed systems into HP SIM or a root CA certificate. Refer to “Trusted Certificates” and “Server Certificates” for complete details.

Certificates

HP SIM allows for secure and authorized management from the central management server (CMS). Users' authorizations for managed systems and the CMS can be configured, helping ensure only authorized users perform state-changing operations. Communication between the CMS, managed systems, and the browser is secured using SSL and certificates, helping to authenticate systems and protect user credentials and management data.

Related Procedures

- Configuring the System Link
- Configuring Login Events

Related Topics

- Server Certificates
- Trusted Certificates
- Users and Authorizations
- About Login
- About Secure Task Execution

About Login

Single Login

Single Login allows a link within an HP Systems Insight Manager (HP SIM) page to establish an authenticated browser session to a managed system that supports Single Login without requiring users to re-enter their user names and passwords. However, if you are trying to establish an authenticated browser session with another instance of HP Systems Insight Manager running on

another system, you must re-enter your user name and password. Single Login links exist wherever there is a link to another system.

Note:



HP SIM is the initial point of authentication, and browsing to another managed system must be from within HP SIM.

If you browse to a managed system using any method other than the links within HP SIM, Single Login is not supported, and you are required to enter the appropriate user name and password for each managed system. Managed systems must be set up to trust an HP SIM system before accepting a Single Login command. Trust is set up at the system by importing the HP SIM system certificate into the Trusted Management Servers List of the system. Refer to “Setting Up Trust Relationships” for more information.

Important:



If you browse to a managed system using any method other than the links within HP SIM, Single Login is not supported, and you are required to enter the appropriate user name and password for each managed system.

Managed Systems must be set up to trust an HP SIM system before accepting a Single Login command. Trust is set up at the system by importing the HP SIM system certificate into the Trusted Management Systems List of the system. Refer to “Requiring Trusted Certificates” for more information.

Note:



Single Login does not work on a Virtual Cluster System. However, it does work on the physical systems which compose the cluster.

Signing In

Signing into HP Systems Insight Manager allows access to HP SIM and determines what authorizations you have in HP SIM. Browsing to HP SIM using Secure Socket Layer (SSL) encrypts all information between the browser and HP SIM, including login credentials. SSL securely encrypts the password and helps prevent someone from capturing and replaying a valid login sequence.

The login page has three fields:

- **User Name.** The name of the user.
- **Password.** The password for the user name.
- **Domain Name.** The Windows domain of the user. This field appears in Windows environments only.

Note:



In a Windows environment, administrators are selected from the operating system during the HP SIM installation. To sign into HP SIM, enter the appropriate information for the account in the fields provided. The **User Name** field specifies the user name, and the **Domain Name** specifies the Windows domain. These fields are required in a Windows environment.

After the credentials are securely received by HP SIM, HP SIM validates the account, verifies that browsing is being done from a valid IP address for that account, and authenticates the credentials against the Windows domain. Refer to “Users and Authorizations” for details about accounts .

Some login failures are caused by failure in the operating system, some by failure within HP SIM. Use the operating system User Management tools to address these potential login failures:

- login credentials are not entered correctly. Passwords are case-sensitive.
- The account being entered has been deleted or has been disabled or locked out.
- The password for the account has expired or must be changed.

The following reasons for login failure within HP SIM can be addressed on the **Users and Authorizations** pages:

- The account being entered is not an account for HP SIM.
- You are attempting to sign in from an IP address that is not valid for the specified account. Finally, the browser systems can also be the cause for login failures.
- Browser not configured to accept cookies.

Note:



Refer to the HP Systems Insight Manager Installation and User Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information.

- A cookie blocker is installed.

Note:



HP SIM can be configured to log an event in the HP SIM Event Database when a login attempt fails or succeeds and when a sign out occurs.

Login Authentication on Linux and HP-UX

HP SIM uses Pluggable Authentication Modules (PAM) to authenticate users who log into the Web server interface on Linux and HP-UX.

Configuring PAM on a Linux System

The administrator of a Linux CMS can customize the PAM that HP SIM uses. The file `/etc/pam.d/mxpamauthrealm` contains the authentication steps for the HP SIM Web server interface. The default for this file is:

- `##PAM-1.0`
- `auth required /lib/security/pam_unix.so`
- `account required /lib/security/pam_unix.so`
- `session required /lib/security/pam_unix.so`

This default setup directs PAM to use the standard UNIX authentication module to authenticate users attempting to log into the HP SIM Web server interface. Standard calls from the system libraries are used to access account information usually read from `/etc/password` or `/etc/shadow`.

The administrator of the system can adjust these requirements to conform to the security requirements of the system. For example, if the security policy on the system is time dependent and `/etc/security/time.conf` is configured, you could adjust `mxpamauthrealm` to:

- `##PAM-1.0`
- `auth required /lib/security/pam_unix.so`
- `account required /lib/security/pam_unix.so`
- `session required /lib/security/pam_unix.so`

Configuring PAM on an HP-UX System

Customizing PAM security on HP-UX is very similar. All of the PAM configurations are stored in `/etc/pam.conf`.

The lines for HP SIM on HP-UX 11i are:

- `mxpamauthrealm auth required /usr/lib/security/libpam_unix.1`
- `mxpamauthrealm account required /usr/lib/security/libpam_unix.1`
- `mxpamauthrealm session required /usr/lib/security/libpam_unix.1`

The lines for HP SIM on HP-UX 11i 2.0 are:

- `mxpamauthrealm auth required /usr/lib/security/$ISA/libpam_unix.1`
- `mxpamauthrealm account required /usr/lib/security/$ISA/libpam_unix.1`
- `mxpamauthrealm session required /usr/lib/security/$ISA/libpam_unix.1`

If you want the HP SIM Web server login model to match what is configured for your other login methods (telnet, rlogin, login, ssh, and so on), configure the same plug-in modules that are used by these other login methods. These should be defined by the **login** service name in the `/etc/pam.conf` file or the `/etc/pam.d/login` file.

Related Topics

- Networking and Security
- About Secure Task Execution
- Installing OpenSSH
- Managing SSH Keys

About Secure Task Execution

HP Systems Insight Manager (HP SIM) tasks that cause state or configuration changes on managed systems use Secure Task Execution (STE) to issue their commands to the system. STE enables an HP SIM system to securely request execution of a task from a managed system. It ensures that the user requesting the task has the appropriate rights to perform the task. The request includes a digital signature to uniquely identify the HP SIM system making the request. Secure Sockets Layer (SSL) is then used to encrypt the request and protect the data from alteration or eavesdropping. Refer to “Setting Up Trust Relationships” for more information.

Note:



STE requires a Trusted Management Servers List at each managed system to ensure that only specified HP SIM systems can execute tasks on the system.

Note:



On the managed system, only Trust by Certificate ensures the request came from the specified HP SIM system. Other options, such as Trust by Name or Trust All, do not verify the digital signature of the HP SIM system and, therefore, cannot reliably verify the sender of the request.

Note:



Tasks using STE, such as Replicate Agent Settings and Install Software and Firmware, do not work against a Virtual Cluster System. However, these tasks work when executed directly against the physical systems of the cluster.

Related Topics

- Exporting a Server Certificate
- Setting Up Trust Relationships

- Requiring Trusted Certificates
- Creating a Server Certificate
- Installing OpenSSH
- Managing SSH Keys

Configuring the System Link

Configure the system link to choose the name format used when creating links to managed systems. The System Link Configuration setting configures how HP Systems Insight Manager (HP SIM) creates browser links to remote systems and how it communicates with remote systems for certain requests.

Note:



When you are browsing to systems using Secure Sockets Layer (SSL), the system name should match the name in the system certificate to prevent browser warnings.

To configure the system link:

1. Click **Options->Security->System Link Configuration**. The **System Link Configuration** page appears.
2. Select from the following options:
 - **Use the system name**. Select this option to use the system name.
 - **Use the system IP address**. Select this option to use the system IP address. For systems with multiple addresses, multiple links might be provided.
 - **Use the system full DNS name**. Select this option to use the full system DNS name.

Note: During discovery, the full system DNS name will be used as the primary lookup key if it is available. Otherwise, the IP address is used.

Note: In the case of systems with multiple network interfaces, selecting the **Use the system name** provides only one link per destination to the system, whereas **Use the system IP address** provides multiple links to the system.

3. Click **OK** to save and apply the changes.

Related Topics

- Networking and Security
- Server Certificates
- Installing OpenSSH
- Managing SSH Keys

Configuring Login Events

Configure login events to create actionable events for login and logout activities.

Note:



This does not affect the HP Systems Insight Manager (HP SIM) Audit Log. These activities are always logged in the HP SIM Audit Log.

To configure login events:

1. Select **Options>Security>Login Event Settings**. The **Login Event Settings** page appears.
2. Select from the following options:
 - **All login and logout activities**. Select this option to create events for all login and logout actions.
 - **Only failed login attempts**. Select this option to create events for only login attempts that are unsuccessful.
 - **None**. Select this option if you do not want to create any events for login or logout activities.
3. Click **OK** to save and apply the changes.

Related Topics

- Networking and Security
- Users and Authorizations
- Installing OpenSSH
- Managing SSH Keys

Configuring Browser Timeout Options

HP Systems Insight Manager (HP SIM) enables you to configure the browser timeout settings to one of the following. These settings affect the browser session while signed in to the HP SIM GUI.

Monitor. When the timeout option is configured to monitor, the HP SIM session remains alive and is continually refreshed, unless you close the browser or navigate to another site. If you close the browser, the session is closed immediately. If you navigate to another site, HP SIM logs you out after 20 minutes. This option is the default, and appears in the `globalsettings.props` file as `EnableSessionKeepAlive=true`.

Active. When the timeout option is configured to remain active, the HP SIM session remains alive as long as you are actively working in HP SIM. However, HP SIM ends your session and logs you out after 20 minutes of inactivity.

You can change the timeout settings to monitor or active by editing the `globalsettings.props` file.

To configure the timeout setting to active:

1. Open the `globalsettings.props` file.

- On a Windows operating system, the `globalsettings.props` file is located in the `install directory/config` folder.
 - On an HP-UX/Linux operating system, the `globalsettings.props` file is located in the `/etc/opt/mx/config` directory.
2. Change `EnableSessionKeepAlive=true` to `EnableSessionKeepAlive=false`.
 3. Click **File->Save**.
The updates are saved.
 4. Close the `globalsettings.props` file.

To change the default timeout:

1. From the HP SIM directory, navigate to `/hpwebadmin/webapps/MxSessionTimeout/WEB-INF/` and open `web.xml`.
2. Edit the minutes from the default of 20 minutes to the number of minutes you want.
3. Save the `globalsettings.Props` and the `web.xml` files.
The updates are saved.
4. Close the `web.xml` file.

Related Topics

- Signing In
- Networking and Security
- Users and Authorizations

Server Certificates

The **Server Certificate** page enables you to view and manage the SSL server certificate of the central management server (CMS). HP Systems Insight Manager (HP SIM) supports two types of certificates, self-signed and Certificate Authority (CA)-signed. A self-signed certificate is created by default during installation, enabling you to browse to HP SIM. The self-signed and CA-signed certificates can be created after installation. The CA-signed certificate requires an internal certificate server or an external CA to sign the certificate.

HP SIM provides the following security certificate options:

- **Export server certificate.** Select **Options->Security->Certificates->Server Certificates**, and then click **Export**.
- **Edit server certificate.** Select **Options->Security->Certificates->Server Certificates**, and then click **Edit**.
- **Create new server certificate.** Select **Options->Security->Certificates->Server Certificates**, and then click **New**.

- **Import server certificate.** Select **Options->Security->Certificates->Server Certificates**, and then click **Import**.

Related Procedures

- Exporting a Server Certificate
- Editing a Server Certificate
- Creating a Server Certificate
- Importing a Server Certificate
- Synchronizing Certificates
- Creating a Certificate Signing Request
- Submitting a Certificate Signing Request
- Importing a CA-Signed Certificate

Related Topics

- Networking and Security
- Replicating Trusted Certificates
- Installing OpenSSH
- Managing SSH Keys

Exporting a Server Certificate

Export the HP Systems Insight Manager (HP SIM) server certificate to a file to facilitate deployment of the certificate into your browsers. This certificate enables a browser to properly identify the HP SIM server and is a public document, so it does not need to be kept private. If the certificate is kept publicly accessible, ensure it cannot be modified.

Note:



The system certificate can be exported as a Base-64 encoded certificate. The exported certificate can be imported into a browser or the Trusted Management Servers List.

To export the server certificates from HP SIM:

1. Select **Options->Security->Certificates->Server Certificates**, and then click **Export**.
The Internet Explorer **File Download** dialog box appears.
2. Click **Save**. You can click **Cancel** to abort the file download operation and return to the **Server Certificate** page. The file is exported and saved.

Related Procedures

- Creating a Server Certificate
- Importing a Server Certificate
- Editing a Server Certificate
- Synchronizing Certificates

Related Topics

- Server Certificates
- Networking and Security
- Installing OpenSSH
- Managing SSH Keys

Editing a Server Certificate

Edit a server certificate to change fields in an existing certificate. This modification might be required if you are submitting a Certificate Signing Request (CSR) to an external Certificate Authority (CA).

Note:



This process also replaces the local System Management Homepage certificate and private key, and updates the certificate sharing directory with a new server certificate and private key.

Note:



Valid characters for each of these fields are a through z (lowercase), A through Z (uppercase), 0 through 9, and the following special characters: ' () + , - . / : ? space _ and ~. Each field must contain at least one non-white space character.

To edit a server certificate:

1. Select **Options->Security->Certificates->Server Certificates**, and then click **Edit**. The **Edit Server Certificate** section appears.
2. Edit the following fields as necessary:

Note: The **Common Name (CN)** field and the key-pair cannot be modified, so the trust relationships with any System Management Homepages remain in tact. However, the browser trust must be re-established by importing the modified certificate and deleting the old certificate from the browser.

- a. In the **Organization (O)** field, enter the name of your organization. This field can be up to 64 characters in length.
- b. In the **Organizational Unit (OU)** field, enter the name of your department. This field can be up to 64 characters in length.
- c. In the **Locality (L)** field, enter the name of your city. This field can be up to 128 characters in length.
- d. In the **State (S)** field, enter the name of your state. This field can be up to 128 characters in length.

- e. In the **Country (C)** field, enter the name of your country. This field can have up to two alphanumeric characters, using the two-letter country codes.
3. Click **OK**. A warning message appears, indicating that the certificate is about to be modified. You can click **Cancel** to abort the modify operation.

Related Procedures

- Creating a Server Certificate
- Exporting a Server Certificate
- Importing a Server Certificate
- Synchronizing Certificates

Related Topics

- Server Certificates
- Networking and Security
- Installing OpenSSH
- Managing SSH Keys

Creating a Server Certificate

Users with full-configuration-rights can create a new self-signed certificate when they must replace the HP Systems Insight Manager (HP SIM) Secure Sockets Layer (SSL) server certificate and private key under the following situations:

- The integrity of the HP SIM server certificate private key is compromised.
- The existing HP SIM server certificate expires.

This self-signed certificate is configured to expire 10 years from its date of creation.

Create a new self-signed certificate when you must replace the HP SIM SSL server certificate and private key. The public key is included in the certificate that goes out to the client. The private key is kept secure in the keystore database on the HP SIM server file system. The public and private key pair of the System Management Homepage (residing on the same system) is overwritten with the new HP SIM public and private key pair.

Important:



Replacing the SSL server certificate and private key invalidates the existing HP SIM server certificate and the System Management Homepage certificate wherever they might be imported, such as browsers and Trusted Management Servers List in other System Management Homepages. Replace the previous server certificate with the new server certificate, in accordance with your security practices, to return to the same level of functionality you had before.

Note:



This process also replaces the local System Management Homepage certificate and private key and updates the certificate sharing directory with a new server certificate and private key.

Note:



Valid characters for each of these fields are a through z (lowercase), A through Z (uppercase), 0 through 9, and the following special characters: ' () + , - . / : ? space _ and ~. Each field must contain at least one non-white space character.

To create a new certificate:

1. Select **Options->Security->Certificates->Server Certificates**, and then click **New**. The **New Server Certificate** section appears and the fields are automatically populated with default values.
2. (Optional) Change the following fields:
 - a. The **Common Name (CN)** field holds the parameter that the browser uses for name comparison when browsing to the central management server. This field can be updated with other name formats, such as fully qualified names and can contain up to 255 characters.
 - b. In the **Organization (O)** field, enter the name of your organization. This field can contain up to 64 characters.
 - c. In the **Organizational Unit (OU)** field, enter the name of your department. This field can contain up to 64 characters.
 - d. In the **Locality (L)** field, enter the name of your city. This field can contain up to 128 characters.
 - e. In the **State (S)** field, enter the name of your state. This field can contain up to 128 characters.
 - f. In the **Country (C)** field, enter the name of your country. This field can contain up to two alphanumeric characters, using the two-letter country codes.
3. After changes are made, click **OK**. If you click **Cancel**, you are returned to the **Server Certificate** page without creating a new server certificate. A warning appears, reminding you of the effects of changing the certificate and private key. If you click **OK** in the warning box to continue, a new 1,024-bit key-pair and a new self-signed certificate are generated. The old key-pair and certificate are not retrievable unless a backup was created manually before this process. The new certificate and private key take effect the next time HP SIM is restarted.

4. Reboot the HP SIM server to ensure the new certificate is properly synchronized with the local System Management Homepage and any applications or components using the certificate sharing directory. After creating a new server certificate, reboot the HP SIM server for the HP SIM server certificate to be synchronized with the HTTP server certificate. Synchronizing the certificates prevents repeated browser security alerts when browsing to HP Insight Management Agent on the HP SIM server.

Related Procedures

- Exporting a Server Certificate
- Importing a Server Certificate
- Editing a Server Certificate
- Synchronizing Certificates

Related Topic

- Server Certificates
- Installing OpenSSH
- Managing SSH Keys

Importing a Server Certificate

Import a Certificate Authority (CA)-signed server certificate to replace the existing server certificate in the following situations:

- You have installed HP Systems Insight Manager (HP SIM) and want to replace the default self-signed certificate with a certificate created by a third-party CA or your own internal CA.
- The integrity of the HP SIM server certificate private key is compromised.
- The existing HP SIM server certificate has expired.

Caution:



Replacing the SSL server certificate and private key invalidates the existing server certificate wherever it might be imported, such as browsers and the Trusted Management Servers Lists of managed systems. Replace the previous server certificate with the new server certificate, in accordance with your security practices, to return to the same level of functionality you had before.

Note:



This process also replaces the local System Management Homepage certificate and private key and updates the certificate sharing directory with a new server certificate and private key.

To import a server certificate:

1. Create a Certificate Signing Request (CSR). Refer to “Creating a Certificate Signing Request”. The CSR uses parameters from the existing certificate. If you want to change those parameters, edit the server certificate (refer to “Editing a Server Certificate”) or create a new server certificate (refer to “Creating a Server Certificate”).
2. Submit the request to a CA. Refer to “Submitting a Certificate Signing Request” for more information. The CA returns a signed certificate.
3. Import the signed certificate reply into HP SIM. Refer to “Importing a CA-Signed Certificate” for more information.

Related Procedures

- Creating a Server Certificate
- Exporting a Server Certificate
- Editing a Server Certificate
- Synchronizing Certificates
- Creating a Certificate Signing Request
- Importing a CA-Signed Certificate
- Submitting a Certificate Signing Request

Related Topics

- Server Certificates
- Networking and Security
- Installing OpenSSH
- Managing SSH Keys

Creating a Certificate Signing Request

Create a Certificate Signing Request (CSR) to replace the HP Systems Insight Manager (HP SIM) Secure Sockets Layer (SSL) server certificate and private key.

To create a certificate signing request:

1. Select **Options->Security->Certificates->Server Certificates**, and then click **Import**. The **Import Server Certificate** section appears.
2. Click **more** next to **Create a Certificate Signing Request (CSR)**.

The **Create Certificate Signing Request** section appears below the **Import Server Certificate** section.

Note: The current certificate parameters are shown. Selecting to create a CSR does not create a new key-pair or change any certificate parameters. If you want to create a new key-pair, create a new certificate. If you want to modify the certificate parameters, click **Edit** instead of **Import** on the **Server Certificate** page.

3. Click **Create** to create a PKCS #10 signing request that is downloaded by way of a standard browser. In Internet Explorer, use the **File Download** dialog box. In Mozilla, save the text in the new browser window to a file.
4. Send the certificate file to a Certificate Authority (CA), which can be internal or external.

Note: The existing self-signed certificate is still valid, so the SSL Web server remains operational for browsing until the signed certificate is received from the CA.

Related Procedures

- Importing a Server Certificate
- Importing a CA-Signed Certificate
- Submitting a Certificate Signing Request

Related Topics

- Server Certificates
- Networking and Security
- Installing OpenSSH
- Managing SSH Keys

Submitting a Certificate Signing Request

After creating the Certificate Signing Request (CSR), the CSR must be submitted to the desired Certificate Authority (CA) for signing.

Note:



You first must complete the Creating a CSR before proceeding with this procedure. Refer to “Creating a Certificate Signing Request” for more information.

To submit request to CA:

1. Select **Options->Security->Certificates->Server Certificates**, and then click **Import**. The **Import Server Certificate** section appears.
2. Click **more** next to **Submit CSR to Certificate Authority (CA)**.
3. Send the PKCS #10 (CSR) data to a CA.

After the CA has returned PKCS #7 data, import it into the HP Systems Insight Manager (HP SIM).

Related Procedures

- Importing a Server Certificate
- Creating a Certificate Signing Request
- Importing a CA-Signed Certificate

Related Topics

- Server Certificates
- Networking and Security
- Installing OpenSSH
- Managing SSH Keys

Importing a CA-Signed Certificate

After creating a Certificate Signing Request (CSR) and having it signed by a Certificate Authority (CA), you can import the signed certificate.

Note:



The only importable certificate format is PKCS #7 formatted certificates. If the certificate reply received from the CA is a single certificate, then first import a self-signed root certificate from the issuing CA into the HP Systems Insight Manager (HP SIM) Trusted System Certificates List. After importing the CA root certificate, the certificate reply can then be imported to serve as the HP SIM server certificate.

Note:



This process also replaces the local System Management Homepage certificate and private key and updates the certificate sharing directory with a new server certificate and private key.

Note:



HP SIM only supports importing certificates that have a public key size of 2046 bits or less.

To import the signed certificate reply from a CA:

1. Select **Options->Security->Certificates->Server Certificates**, and then click **Import**. The **Import Server Certificate** section appears.
2. Click **more** next to **Import signed certificate reply from CA**. The **Import Signed Certificate Reply** section appears below the **Import Server Certificate** section.
3. Click **Browse** next to the **Certificate filename** field. The **Choose file** dialog box appears.
 - a. Navigate to the location where the signed certificate is stored.
 - b. Select the correct filename, and click **Open**.

The file name appears in the **Certificate filename** field.

4. Click **Import**. The signed certificate is imported.

After creating a CSR or importing the server certificate, reboot the HP SIM server for the HP SIM server certificate to be synchronized with the System Management Homepage certificate and the certificate sharing directory. Synchronizing the certificates prevents repeated browser

security alerts when browsing to HP Insight Management Agent on the HP SIM server, which allows the HP SIM and the local System Management Homepage to update their Secure Sockets Layer (SSL) server certificates and private keys.

Related Procedures

- Importing a Server Certificate
- Creating a Certificate Signing Request
- Submitting a Certificate Signing Request

Related Topics

- Server Certificates
- Networking and Security
- Installing OpenSSH
- Managing SSH Keys

Synchronizing Certificates

When the HP Systems Insight Manager server certificate is created or modified, the public and private key pair of the System Management Homepage certificate is overwritten with the HP Systems Insight Manager public and private key pair.

Note:



This feature is available in the unlikely event that the certificates become unsynchronized for an unknown reason.

Note:



For the certificate sharing feature to work in HP-UX, OpenSSL must be installed in the `/OPT/APACHE/SSL/BIN/` directory (default for HP-UX installs). For the certificate sharing feature to work in Linux, OpenSSL must be installed in the `/USR/BIN/` directory (default for Linux installs).

Related Procedures

- Creating a Server Certificate
- Exporting a Server Certificate
- Importing a Server Certificate
- Editing a Server Certificate

Related Topics

- Server Certificates
- Networking and Security
- Replicating Trusted Certificates

- Installing OpenSSH
- Managing SSH Keys

Replicating Trusted Certificates

System Administrators that have the HP Systems Insight Manager (HP SIM) **Require Trusted Certificates** feature enabled can replicate the trusted certificates list to other HP SIM systems. If you do not use the Require Trusted Certificates feature of the HP SIM for a two-way trust solution, this is not necessary.

Migrating Trusted System Certificates from the Source CMS to the Target CMS

There are two options available to migrate the trusted certificates from a source central management server (CMS) to a target CMS. The first option can be used when the source CMS has large number of trusted certificates and the second option can be used when a source CMS has a lower number of trusted certificates.

Migrating certificates when the source CMS has a large number of trusted certificates

Warning: You will lose the existing SSL Server Key and certificate on the target CMS and must re-establish the trust relationship with any agents configured to trust the target CMS. Refer to Step 13.

1. Sign into HP SIM on the source CMS system with administrative privileges.
2. Go to `<HPSIM Install folder>\Systems Insight Manager\config\certstor.`
3. Copy the files named `hp.keystore` and `keyfile.3`.
4. Log into the target CMS system with administrative privileges.
5. Go to the `<HPSIM Install folder>\Systems Insight Manager\config\certstor` directory.
6. Replace `hp.keystore` and `keyfile.3` files with the files copied.
7. On the target CMS system, go to **Start->Settings->Control Panel->Administrative Tools->Services**.
8. Restart the HP SIM service.

Note: You may see a browser warning indicating the name in the certificate does not match the name of the site. This is expected since you are temporarily using the certificate from the source CMS, but you can view the certificate displayed by the browser to ensure its authenticity before logging in.

9. Sign into HP SIM on the target CMS with administrative privileges. Go to **Options->Security->Certificates->Server Certificate**.
10. Click **New** and create a new server certificate.

11. On the target CMS system, go to **Start->Settings->Control Panel->Administrative Tools->Services**.
12. Restart the HP SIM service.
13. Install the new server certificate to required managed systems using the Replicate Agent Settings feature. For more information, refer to “Replicating the Trusted Certificates and Trust Mode from the Source CMS to Trusted Managed Systems using the Replicate Agent Settings Feature”.

Migrating certificates when the source CMS has a lower number of trusted certificates

1. Log into the source CMS system with administrative privileges.
2. Go to **Options->Security->Certificates->Trusted Certificate**.
3. Select a certificate and click **Export**.
4. Save the certificate locally.
5. Repeat the steps 2 and 3 for all certificates listed on the **Trusted System Certificates** page.
6. Copy all exported certificates to the target CMS system.
7. Sign into HP SIM on the target CMS with administrative privileges.
8. Go to **Options->Security->Certificates->Trusted Certificate**.
9. Click **Import**.
10. Click **Browse** and select a certificate.
11. Click **OK**.
12. Repeat the last three steps for all certificates.

Replicating the Trusted Certificates and Trust Mode from the Source CMS to Trusted Managed Systems using the Replicate Agent Settings Feature

Note:



This section assumes the agents are already configured to trust the source CMS.

Note:



This configures the agents to trust only the new target CMS. If trust for the original source CMS is still desired, duplicate steps 5, 6, and 13 (or 16) using the source CMS.

1. Log into the System Management Homepage on the target CMS.
2. Go to **Settings->Security->Trust Mode**.
3. Select **Trust by Certificate** and click **Save Configuration**.
4. Go to **Settings->Security->Trusted Management Servers**.
5. Enter the IP address of the target CMS in the field adjacent to **Add Certificate From Server**.
6. Click **Add Certificate From Server**.
7. Sign into HP SIM on the source CMS with administrative privileges.
8. Go to **Configure->Replicate Agent Settings**.
9. From **Select Target Systems** page, select all managed systems that are configured to trust the source CMS.
10. Click **Apply Selections** and click **Next**.
11. Select the target CMS as source and click **Next**.
Note: If the source system does not have HP SIM, skip to step 15.
12. In the source configuration settings page, go to **System Management Homepage->Settings->Configuration Options Properties** and select **Trust Mode**.
13. Go to **System Management Homepage->Settings->Trusted Certificate Properties** and select **Trusted Certificate** of the target CMS.
14. In the source configuration settings page, go to **HTTP Server->Configuration->Options Properties** and select **Trust Mode**.
15. Go to **HTTP Server->Trusted Certificates Properties** and select **Trusted Certificate** of the target CMS.
16. Click **Run Now**. The CMS certificates are replicated on the selected managed systems.

Related Procedures

- Creating a Replicate Agent Settings Task
- Exporting a Server Certificate
- Editing a Server Certificate
- Creating a Server Certificate
- Importing a Server Certificate
- Synchronizing Certificates

- Creating a Certificate Signing Request
- Submitting a Certificate Signing Request
- Importing a CA-Signed Certificate

Related Topic

- Networking and Security
- Installing OpenSSH
- Managing SSH Keys

Trusted Certificates

Trusted certificates provide the highest level of security. Users with full-configuration-rights can import certificates from other systems into the HP Systems Insight Manager (HP SIM) Trusted System Certificates List.

The purpose of the Trusted System Certificates List in HP Systems Insight Manager is to maintain a list of certificates in the HP SIM keystore. Certificates include the HP SIM system certificate and the certificates of managed systems that are trusted by the HP SIM system. These imported certificates are placed in the keystore and are displayed in the Trusted System Certificates List.

The list of certificates is used when Require Trusted Certificates is enabled, however the list is manageable regardless of the Require Trusted Certificates state. It can include the certificate itself or a signing certificate if available. Using a signing certificate simplifies the management of the list, because any certificate signed by the signing certificate is valid and trusted. Refer to “Requiring Trusted Certificates” for more information.

HP SIM provides the following trusted certificate options:

- **Import trusted certificate.** Select **Options->Security->Certificates->Trusted Certificates->[Import]**.
- **Export certificate.** Select **Options->Security->Certificates->Trusted Certificates**, and then click **Export**.
- **Delete trusted certificate.** Select **Options->Security->Certificates->Trusted Certificates**. Select the certificates to be deleted and click **Delete**.

Related Procedures

- Importing Trusted Certificates
- Exporting Trusted Certificates
- Deleting Trusted Certificates

Related Topics

- Requiring Trusted Certificates
- Administering Systems and Events
- Server Certificates
- Requiring Trusted Certificates
- Setting Up Trust Relationships
- Replicating Trusted Certificates
- Installing OpenSSH

- Managing SSH Keys

Importing Trusted Certificates

If you have selected **Require trusted certificates** on the **Trusted System Certificates** page, you must import certificates that represent the managed systems you want to trust into the Trusted Certificates List. You can import the certificate of the system itself on a per system basis. You can also import the signing certificate of the Certificate Authority (CA) or intermediate CA used to sign and issue certificates for groups of systems, which simplifies the maintenance of this list.

Note:



Only users with full-configuration-rights can import certificates into the HP Systems Insight Manager (HP SIM) Trusted System Certificates List.

Note:



HP SIM only supports importing certificates that have public key sizes of 2,048 bits or less.

To import certificates into the Trusted System Certificates List:

1. Select **Options->Security->Certificates->Trusted Certificates**, and then click **Import**. The **Import Trusted System Certificate** section appears.
2. Next to the **Certificate filename** field, click **Browse**.
The **Choose file** dialog box appears.
3. Navigate to the location of the certificate to be imported, and select the file name. Click **Open**.
The certificate is imported.

Related Procedures

- Trusted Certificates
- Exporting Trusted Certificates
- Deleting Trusted Certificates

Related Topics

- Trusted Certificates
- Setting Up Trust Relationships
- Server Certificates
- Networking and Security
- Installing OpenSSH
- Managing SSH Keys

Exporting Trusted Certificates

Export the HP Systems Insight Manager (HP SIM) server certificate to a file to facilitate deployment of the certificate into your browser, enabling a browser to properly identify the HP SIM server. This certificate is a public document, so it does not need to be kept private. If the certificate is kept publicly accessible, ensure it cannot be modified.

Only HP SIM users with full-configuration-rights can export the HP SIM system certificate from HP SIM.

Note:



The system certificate can be exported as a Base-64 encoded certificate. The exported certificate can be imported into a browser or the Trusted Management Systems List of a system.

Exporting the System Certificate From HP SIM

To export the system certificate from HP SIM using Microsoft Explorer:

1. Select **Options->Security->Certificates->Trusted Certificates**, and then click **Export**.
The **File Download** dialog box appears.
2. Select the location for the file to be saved.
3. Enter a file name and click **Save** to save the certificate as a Base-64 encoded X.509 certificate. This file can be imported into a browser or managed system for authentication of the central management server (CMS) during an Secure Sockets Layer (SSL) connection. You can click **Cancel** to abort the save operation and return to the **System Certificate** page.

To export the system certificate from HP SIM using Mozilla:

1. Display the certificate in a new browser window.
2. Select the entire contents of the browser window that includes the certificate.
3. Copy the selected text to the clipboard.
4. Paste the text to your favorite text editor, and save the file with a **.CER** file extension.

Exporting the System Certificate from the Browser (Microsoft Internet Explorer Only)

1. View the HP SIM system certificate, using one of the following methods:
 - From the Internet Explorer browser menu, select **File->Properties->Certificates**.
 - Double-click the **Lock** icon in the lower right portion of the browser to display the **Certificate** dialog box.

The **Certificate** dialog box appears.

2. Select the **Details** tab in the **Certificate** dialog box.
The **Details** tab appears.
3. Click **Copy to File**.
The Certificate Export Wizard is launched.
4. Click **Next**.
The **Export File Format** dialog box appears.
5. Select **Base-64 encoded X.509** for the export file format. Click **Next**.
The **File to Export** dialog box appears.
6. In the **File name** field, enter the file you want to export. Click **Next**.
The **Completing the Certificate Export Wizard** dialog box appears.
7. Click **Finish**. You can click **Back** to return to the previous page or click **Cancel** to abort the export operation.
A message appears, indicating the export is completed.
8. Click **OK**.

Related Procedures

- Trusted Certificates
- Importing Trusted Certificates
- Deleting Trusted Certificates

Related Topics

- Trusted Certificates
- Setting Up Trust Relationships
- Server Certificates
- Networking and Security
- Installing OpenSSH
- Managing SSH Keys

Deleting Trusted Certificates

Delete certificates from the Trusted System Certificates List to remove them from the HP Systems Insight Manager (HP SIM) keystore.

Caution:



The delete process is irreversible. Use this feature with caution!

To delete certificates from the Trusted System Certificates List:

1. Select **Options->Security->Certificates->Trusted Certificates**.
2. Select the certificates to be deleted.
3. Click **Delete**. A dialog box appears.
4. Click **Yes** to delete the certificates, or click **Cancel** to abort the delete process and return to the **Trusted System Certificates** page.

The certificates are deleted from the Trusted System Certificates List.

Related Procedures

- Importing Trusted Certificates
- Exporting Trusted Certificates
- Requiring Trusted Certificates

Related Topics

- Trusted Certificates
- Server Certificates
- Networking and Security
- Installing OpenSSH
- Managing SSH Keys

Requiring Trusted Certificates

Trusted system certificates are certificates that represent managed systems. Enabling the **Require trusted certificates** option on the **Trusted System Certificates** page allows HP Systems Insight Manager (HP SIM) to authenticate the remote managed system. For ease of use, this option is disabled, which is the typical scenario, and maintains a high level of security. For maximum security, this option should be enabled, which requires some extra configuration.

If **Require trusted certificates** is enabled, when HP SIM attempts to make a Secure Sockets Layer (SSL) connection to a managed system, a certificate representing that system must be found in the HP SIM keystore or the SSL connection fails, and the attempted operation fails as well. The certificate representing the system can be the system SSL system certificate, or the Certificate Authority (CA) level certificate that was used to sign the system certificate. For many systems, having a handful of CA level certificates sign all the system certificates can simplify the management and maintenance of the system certificates. However, this option requires the presence of a Public Key Infrastructure (PKI) in your environment or the services of a third-party security company.

Caution:



If you select the **Require trusted certificates** option, a warning message appears indicating that certain features work only for systems whose certificates are represented in the Trusted System Certificates List.

Note:



The HP SIM Trusted System Certificates list is only used when **Require trusted certificates** is enabled.

Note:



Changing the **Require trusted certificates** option can adversely affect the operation of HP SIM. Carefully read and understand the displayed warning as described below.

Note:



When using a CA level certificate, any valid certificate signed by the CA level certificate is accepted by HP SIM, whether it is already issued or issued at some point in the future.

Related Procedures

- Importing Trusted Certificates
- Exporting Trusted Certificates
- Deleting Trusted Certificates

Related Topic

- Trusted Certificates
- Setting Up Trust Relationships
- Installing OpenSSH
- Managing SSH Keys

Setting Up Trust Relationships

How to set up a trust relationship between an HP Systems Insight Manager (HP SIM) CMS and a managed Windows server having ProLiant Agents installed.

Setting up the CMS to Trust Managed ProLiant Servers

1. In HP SIM, select **Options->Security->Certificates->Server Certificates**, and then click **Export**. Remember the location of the file (`servcert.cert`).
2. (Optional) In HP SIM, select **Options->Security->Certificates->Trusted Certificates**, and then click **Import**. Locate and import the file which was exported in step 1.

Note:



HP SIM uses the same keystore for the server certificate and trusted certificate.

3. In Internet Explorer, select **Tools->Internet Options->Content->Certificates** and select the **Trusted Root Certificate Authorities** tab. Import the exported file in step 1 and select **Automatically select the certificate store...**

Configuration at the Managed System

For Single Login and Secure Task Execution (STE) to work, the managed system must be running a supported agent and be configured to trust the HP SIM server. The Trust Mode is configured in System Management Homepage.

Trust By Certificate. The **Trust by Certificate** mode sets the **System Management Homepage** to accept configuration changes only from HP SIM servers with trusted certificates. This mode requires the submitted server to provide authentication by means of a digital signature and certificates. This mode is the strongest method of security since it verifies the digital signature before allowing access. HP recommends this option.

Note:



If you do not want to enable any remote configuration changes by HP SIM, leave **Trust by Certificate** selected, and leave the list of trusted systems empty.

Trust By Name. The **Trust By Name** mode sets the **System Management Homepage** to accept certain configuration changes only from servers with the HP SIM names designated in the **Trust By Name** field. The **Trust By Name** option is easy to configure, and prevents non-malicious access. For example, you might use this option if you have a secure network with two separate groups of administrators in two separate divisions. It prevents one group from installing software to the wrong system. This option verifies only the HP SIM server name submitted, not the digital signature.

Trust All. The **Trust All** mode sets the **System Management Homepage** to accept configuration changes from any system. For example, you could use the **Trust All** option if you have a secure network, and everyone in the network is trusted.

Note:



For **Trust By Certificate**, the certificate from the HP SIM system can be installed during the initial support pack deployment. Refer to "Initial ProLiant Support Pack Install" for more information.

Setting Up the Managed Server Running System Management Homepage

1. From a browser, open IE and browse to the managed server through **https://managed-server:2381**. The **System Management Homepage** appears.
2. Log into the **System Management Homepage**.
3. Select **Settings->System Management Homepage->Security**.
4. Click **Trust Mode**. The **Trust Mode** page appears.
5. Select **Trust by Certificate** to Require trusted certificates.
6. Click **Trust Certificate** to access the Trusted Management server certificate.
7. Click **Save Configuration** to save the trust mode, or click **Reset Values** to cancel all changes.
8. Click the browser **Back** button.
9. In the text box, next to **Add Certificate From Server**, enter the name of the HP SIM server that contains the certificate to be added.
10. Click **Add Certificate From Server**. The certificate information is presented for verification before it is added to the list.

Note: Because this is a non-secure request over http, a malicious party could intercept the request and substitute a bogus certificate in response to the request. A more secure method for obtaining the HP SIM Certificate is described in "Importing the HP SIM Certificate" for more information.

11. Verify the certificate information, and if you want to add it to the Trusted Certificate List, click **Add Certificate to Trust List**.

Note: If you are setting up a trusted certificate on a cluster, refer to "Cluster" for more information.

Importing the HP SIM Certificate

1. Export the HP SIM server certificate from the HP SIM server to a file. Refer to "Exporting a Server Certificate" for more information.
2. Place the certificate file in a file location that is accessible to the file system of the managed system.
3. Browse to the managed system and using Notepad, open the HP SIM server certificate created in step 1.
4. Highlight the entire contents of the file, including the **Begin Certificate** and **End Certificate** lines. Copy the highlighted contents of the certificate file to the clipboard.
5. Return to the managed system browser and select the **HP SIM Certificate Data** box.
6. Paste the contents of the certificate file into this box and click **Add Cert** underneath the box. A confirmation window appears with three links at the top.

7. Click **Options** and scroll down to the **Trusted Certificates** section. There is now a list called **Trusted Certificates**: with the server name and two links: **View Certificate** and **Remove Certificate**, for the HP SIM Certificate that was just added.

Configuring HP SIM

1. In Internet Explorer, select **Tools->Internet Options->Content->Certificates** and select the **Trusted Root Certificate Authorities** tab. Import the exported file and select **Automatically select the certificate store....**
2. (Optional) In HP SIM, select **Options->Security->Certificates->Trusted Certificates**, and then click **Import**. Locate and import the file which was exported in Step 1.

Note:



HP SIM uses the same keystore for the server certificate and trusted certificate.

3. Open HP SIM and select **Options->Security->Certificates->Trusted Certificates**, and enable the **Require trusted certificates** option.

Setting Up the Managed Server Running Management HTTP Server

Importing the HP SIM Certificate

1. Export the HP SIM server certificate from the HP SIM server to a file. Refer to “Exporting a Server Certificate” for more information.
2. Place the certificate file in a file location that is accessible to the file system of the managed system.
3. Browse to the managed system and using Notepad, open the HP SIM server certificate created in step 1.
4. Highlight the entire contents of the file, including the **Begin Certificate** and **End Certificate** lines. Copy the highlighted contents of the certificate file to the clipboard.
5. Return to the managed system browser and select the **HP SIM Certificate Data** box.
6. Paste the contents of the certificate file into this box and click **Add Cert** underneath the box. A confirmation window appears with three links at the top.
7. Click **Options** and scroll down to the **Trusted Certificates** section. There is now a list called **Trusted Certificates**: with the server name and two links: **View Certificate** and **Remove Certificate**, for the HP SIM Certificate that was just added.

Requesting the HP SIM Certificate

Enter the HP SIM server name in the appropriate field, and click the corresponding **Get Cert** button. The managed system makes an HTTP request directly to the HP SIM server for its certificate.

Note: Because this is a non-secure request over http, a malicious party could intercept the request and substitute a bogus certificate in response to the request. A more secure method for obtaining the HP SIM Certificate is described in “Importing the HP SIM Certificate” for more information.

Configuration at HP SIM

System Identification

A System Identification Task must be run at least once against any managed system for HP SIM to know that it supports Single Login and Secure Task Execution, or these features will not work.

Certificates for Trusted Systems

If you have enabled **Require trusted certificates** on the **Trusted System Certificates** page (select **Options->Security->Certificates->Trusted Certificate**), import certificates that represent the managed systems you want the HP SIM server to trust into the Trusted System Certificates List of HP SIM. For the managed device certificate, you can use its certificate, or, if applicable, the certificate the Certificate Authority (CA) used to sign the system certificate.

Note:



If **Require trusted certificates** is disabled, the Trusted System Certificates List is not used, and you may omit this section.

Before importing system certificates into the HP SIM Trusted System Certificates List, export the certificates to a file in DER or Base-64 encoded format. For obtaining the system certificate, you can:

- For systems running Windows for which you have access to the file system, copy the certificate in the file `c:\compaq\wbem\cert.pem` in Base-64 encoded format, to somewhere accessible by HP SIM or access it directly, if it is already accessible by HP SIM.
- Export the system certificate while browsing to the system. Select **File->Properties** from the browser menu. Click **Certificates**. Select the **Details** tab, then, click **Copy to File**. Export the certificate as a Base-64 encoded X.509 file.

For obtaining the CA certificate, contact your CA, or, refer to documentation provided with your certificate server software. To import managed system certificates into the HP SIM Trusted System Certificates List:

1. Select **Options->Security->Certificates->Trusted Certificates**, and then click **Import**.
2. The **Import Trusted System Certificate** section appears.
3. Next to the **Certificate Filename** field, click **Browse**.
The **Choose file** dialog box appears.
4. Navigate to the location of the certificate to be imported, and select the file name. Click **Open**.
The certificate is imported.

Note: If you are setting up a trusted certificate on a cluster, refer to “Cluster” for more information.

Managing Browser Warning Messages

To have the browser warning messages stop displaying on the browser:

1. From the browser, open Internet Explorer and browse to the managed server by **https://managed_server:2381**.
2. On the Internet Explorer **Security Alert**, click **View Certificate**.
3. After reviewing the certificate, click **Install Certificate**.
4. Click **Next**.
5. Click **Place all certificates in the following store**.
6. Click **Browse**.
7. Select **Trusted Root Certificate Authorities** and click **OK**.
8. Click **Next**.
9. Click **Finish**.
10. Click **OK**.

Related Procedures

- Creating a Certificate Signing Request
- Submitting a Certificate Signing Request
- Importing a CA-Signed Certificate
- Exporting a Server Certificate
- Setting Up Managed Systems

Related Topics

- Server Certificates
- Trusted Certificates
- Networking and Security
- Creating a Replicate Agent Settings Task
- Installing OpenSSH
- Managing SSH Keys

Monitoring Systems, Clusters, and Events

You can monitor systems, clusters, and events using the tools in the **Systems and Events** panel. It enables you to drill down to locate more information about systems and events and quickly select systems before performing a task. From this panel, you can quickly access the **System Overview** page, the **All Systems** page, and the **All Events** page. You can also save searches in private collections under **Systems** or **Events**. Refer to “Saving Collections” for more information.

Note:



If you upgraded from HP Systems Insight Manager (HP SIM) 4.x to HP SIM 5.0 and you utilized the My Favorites feature, the My Favorites sub-folders and their contents are migrated under the **Private** collections.

About Collections

A collection groups systems into a collection based on information in the HP SIM database. After a collection is defined, you can display the results or associate it with a task. You can save edited or an unedited collection as a collection with another name.

Creating logical collections of systems, clusters, or events reduces the number of systems, clusters, or events viewed in a particular collection. For example, your organization might have five system administrators who are responsible for 100 different systems in six different buildings. You can create a collection for each administrator that includes only their systems, or you can create a collection for each building that includes only the systems located in that particular building.

Complex collections that contain individual collections or a number or search criteria take more system resources to run. Keep the collection as simple as possible to minimize the performance impacts of individual tasks.

Related Procedures

- Customizing the Cluster Table View Page
- Deleting Clusters from the Database
- Printing a Cluster Collection Report
- Entering Comments on Events
- Assigning Events to Users
- Clearing Events from the Collection
- Customizing the Event Table View Page
- Deleting Events from the Database
- Printing an Event Collection Report
- Setting Properties for an Event Collection
- Creating Event Collections
- Performing an Advanced Search for Events
- Deleting Event Collections
- Editing Event Collections

- Setting Properties for a System or Cluster Collection
- Creating System or Cluster Collections
- Performing an Advanced Search for Systems
- Deleting System or Cluster Collections
- Editing System or Cluster Collections
- Performing a Basic Search
- Performing an Advanced Search for Clusters
- Saving Collections
- Customizing the System Table View Page
- Deleting Systems from the Database
- Printing a System Collection Report
- Saving Collections

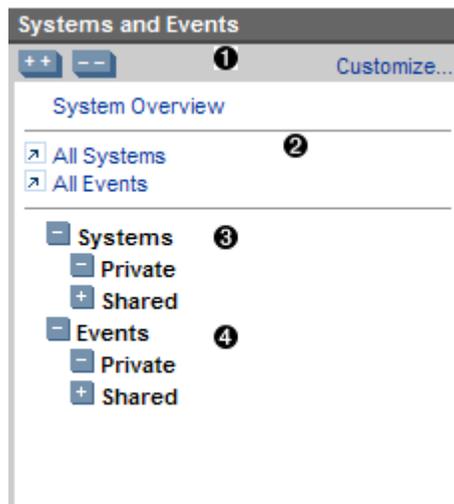
Related Topics

- System Table View Page
- Cluster Table View Page
- Event Table View Page
- Customizing Event Collections
- Customizing System or Cluster Collections
- Searching for Systems and Events
- Viewing the System Overview Page
- Navigating the Systems and Events Panel
- Reference
- Default Public Collections
- Service Notification Events

Navigating the Systems and Events Panel

The **Systems and Events** panel contains the following features:

1. Tree Controls and Customization
2. Overviews
3. Systems
4. Events



Selecting a collection displays a view of its contents. Several types of collection view pages can be launched from the **Systems and Events** panel. Select one of the pages in the list below to view more information several of the different types of views available.

- Navigating the System Table View Page
- Navigating the Event Table View Page
- Navigating the Cluster Table View Page
- Navigating the Picture View Page
- Navigating the Tree View

In the **Systems and Events** panel, the **Private** and **Shared** collections are created by default. Collections in **Shared** can be viewed by any valid HP Systems Insight Manager (HP SIM) user. However, only users with full-configuration-rights can edit or delete these collections and their contents. Collections in **Private** can only be viewed, edited, or deleted by the creator of the collection. Collections can be placed in **Private** or **Shared** collections. To place collections in **Shared**, you must have full-configuration-rights.

If the same collection is placed in both **Shared** and **Private**, any users that have full-configuration-rights can modify the collection stored in the **Shared** collection. When the collection is modified in place, changes are reflected to the other collection. If the user that created the collection has their user rights reduced to limited configuration rights from full-configuration-rights, the user can no longer modify the collection that is located in the **Shared** collection.

Collections and members of collections can be set to not visible. You might want to do this to remove clutter of unused collection from the **Systems and Events** panel. Refer to “Setting Properties for a System or Cluster Collection” and “Setting Properties for an Event Collection” for more information.

Tree Controls and Customization

There are controls available to navigate the tree in the **Systems and Events** panel.

 Used to expand all branches of the tree

 Used to collapse all branches of the tree to first level branches

 Used to expand a branch of the tree

 Used to collapse a branch of the tree

The **Customize** link in the **Systems and Events** panel enables you to customize the **Systems and Events** panel tree to your own preference. Any user can customize his or her own **Systems**, **Events**, and **My Favorites** collections, but only the user who has full-configuration-rights can customize the public **Systems** and **Events** collections. Click **Customize** to display the **Customize Collections** section.

Overviews

The three overview collections in the **Systems and Events** panel include:

- **System Overview**. Displays the **System Overview** page. Refer to “Viewing the System Overview Page” for more information.

- **Health Status.** Contains the health status of all systems discovered by HP SIM. Systems are grouped by their status condition and type. Each number in a column is a hyperlink to a subset of system status collections that belong to this **Health Status** collection.
- **Uncleared Event Status.** Lists the number of uncleared events that have a Critical, Major, Minor, Warning, Normal, or Informational severity. Events are grouped by their severity and system type. Each number in a column is a hyperlink to a more detailed list of events that belong to this **Event Status** lists.

Both displays are sorted using the following System Categories:

- **Servers.** HP servers with HP Insight Management Agents
- **Clusters.** Groups of systems, typically servers
- **Clients.** Workstations, portables, and desktops
- **Networking.** Routers, switches, repeaters, or remote access products
- **Printers.**
- **Other.** Includes Remote Insight boards, third-party systems that do not fit the servers, clusters, clients, or other networking categories, such as racks, enclosures, or remote management processors

Note:



With the use of System Type Manager, other third-party systems can fall into these system types. Refer to “Manage System Types” for more information.

- **All Systems.** Displays the **All Systems** page. Refer to “Navigating the System Table View Page” for information on the system table view page.
- **All Events.** Displays the **All Events** page. Refer to “Navigating the Event Table View Page” for information on the event table view page.

Systems

A system collection logically groups systems into a group based on information in the HP SIM database. After a collection is defined, you can display the results in the workspace or associate it with a management task.

In addition to using the collections provided by HP SIM, you can create, edit, or delete your own collections. Collections must follow specific naming conventions. Refer to “Collection Naming Conventions” for more information on naming collections.

Creating logical groups of systems reduces the number of systems viewed in a particular system list. For example, your organization might have five system administrators who are responsible for 100 different systems in six different buildings. You can create a collection for each administrator that includes only their systems or you can create a collection for each building that includes only the systems located in a particular building.

Complex collections that contain individual systems selections or numerous search criteria take more system resources to run. Keep the collection as simple as possible to minimize the performance impacts of individual tasks. Refer to “Default Public Collections” for a list of all public system collections.

Collections can be grouped together into **Private** collections that you create. **Private** collections of logged-in users are run internally by HP SIM to produce status. You can only access the **Private** collections that you create and not those created by another user.

Events

An event collection logically groups events into a collection based on information in the HP SIM database. Creating logical groups of events reduces the number of events viewed in a particular event collection. After a collection is defined, you can display the results in the workspace or associate it with a management task.

Complex collections that contain individual system selections or numerous selection criteria take more system resources to run. Keep the collection as simple as possible to minimize the performance impacts of individual tasks. Refer to “Default Public Collections” for a list of all shared event collections.

Related Procedures

- Customizing System or Cluster Collections
- Customizing Event Collections

Related Topics

- Monitoring Systems, Clusters, and Events
- Navigating the Tree View
- Viewing the System Overview Page
- System Types

Viewing the System Overview Page

By clicking **System Overview** in the **Systems and Events** panel, you can view the current system health status and uncleared event status. This page does not automatically refresh, but you can refresh the data by clicking the **Last Update** link at the bottom of the page.

Health Status

The Health Status table contains the health status of all systems discovered by HP Systems Insight Manager (HP SIM) that you are authorized to see. Systems are grouped by their status condition and type. Each number in a column is a hyperlink to a subset of system status collections that belong to the System by Status collection.

Uncleared Event Status

You can also view the current status of uncleared events. The Uncleared Event Status table lists the number of uncleared events, for systems you have authorization to see, that have a Critical, Major, Minor, Warning, Normal, or Informational severity. Events are grouped by their severity and system

type. Each number in a column is a hyperlink to a more detailed collection of events that belong to the Event Status collection.

Both displays are sorted using the following system categories:

- **Servers.** HP servers with HP Insight Management Agent
- **Clusters.** Clusters comprised of a group of systems, typically servers
- **Clients.** Workstations, portables, and desktops
- **Networking.** Routers, switches, repeaters, or remote access products
- **Printers.**
- **Other items.** Includes Remote Insight boards, third-party systems that do not fit the servers, clusters, clients, printers, or other networking categories, such as racks, enclosures, or remote management processors

Note:



With the use of System Type Manager, other third-party systems can fall into these system types. Refer to “Manage System Types” for more information on System Type Manager.

Related Topics

- Monitoring Systems, Clusters, and Events
- Navigating the Systems and Events Panel
- Navigating the Event Table View Page
- Navigating the System Table View Page
- Event Severity Types
- System Types

Saving Collections

Perform this procedure to save a system, event, or cluster collection with a new name or to a specific location.

Note:



For a system search, the name can contain no more than 70 characters, must be unique so a duplicate collection name cannot be assigned to the new collection, and include no special characters.

To save a collection:

1. In the **Name** field, enter a name for the collection.

2. Under **Place in Folder**, select where to save the collection (in a **Private** folder of one of the **Shared** folders).
3. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.

Related Procedures

- Performing an Advanced Search for Systems
- Performing an Advanced Search for Events
- Performing an Advanced Search for Clusters
- Performing a Basic Search
- Customizing the System Table View Page
- Deleting Systems from the Database
- Printing a System Collection Report
- Customizing the Cluster Table View Page
- Deleting Clusters from the Database
- Printing a Cluster Collection Report

Related Topics

- Searching for Systems and Events
- Basic and Advanced Search
- Search Criteria
- System Table View Page
- Cluster Table View Page

Customizing System or Cluster Collections

The **Systems and Events** panel contains a **Systems** collection. This collection contains collections of systems, clusters, and **System Functions**.

Collections can be private or shared. Shared collections are visible to all users, and private collections are personal collections you create that only you can view. HP Systems Insight Manager (HP SIM) ships with several predefined shared collections. For example, Systems by Status is a default shared collection that ships with HP SIM. Refer to “Shared System Collections” for information on default shared collections.

- There are two access levels for the system collections: **Shared** and **Private**. All of the default system collections for **Systems**, **Clusters**, and **System Functions** are shared. Refer to “Shared System Collections” for more information on default shared collections.
- Every valid user can view and edit his or her own private collections.
- Every valid user can view shared collections, but users who have full-configuration-rights can modify the content of shared collections. After the modification is complete, every valid user can see the changes.
- Clicking a system or cluster collection name from the **Systems** collection displays the current members of that collection in the workspace area of the page.
- Clicking a cluster collection from the **Systems** collection displays the result of running the selected cluster collection in the workspace area of the page. Refer to “Navigating the Cluster Table View Page” for detailed information on the cluster view page.

To customize system collections, click **Customize** under the **Systems and Events** panel, and the **Customize Collections** page appears. In the **Show** dropdown list, select **Systems**. All available **Systems** are displayed. A table appears that includes the collection name, if the collection is displayed in the **Systems and Events** panel, and if the system status is displayed in the **Systems and Events** panel. Click  to expand all system and cluster collections in the table, or click  to collapse all system and cluster collections in the table.

On the **Customize Collections** page, the following options are available:

- **New.** Used to create a new system or cluster collection. With full-configuration-rights, you can save the new collection as a shared collection. Otherwise, you can only save it as a private collection. Refer to “Performing an Advanced Search for Systems” for more information on creating a system list.
- **Edit.** Used to edit an existing system or cluster collection. Refer to “Editing System or Cluster Collections” for more information.
- **Delete.** Used to delete an existing system or cluster collection. With full-configuration-rights, you can delete a shared system or cluster collection. Only empty system collections can be deleted. To delete an existing collection, highlight the collection and click **Delete**. A dialog box appears. Click **OK** to continue with the deletion, or click **Cancel** to cancel the deletion. Refer to “Deleting System or Cluster Collections” for more information.
- **Set Properties.** Used to set the display status flag, hidden flag, and the default view. Refer to “Setting Properties for a System or Cluster Collection” for more information.

Related Procedures

- Performing an Advanced Search for Systems
- Editing System or Cluster Collections
- Creating System or Cluster Collections
- Deleting System or Cluster Collections
- Setting Properties for a System or Cluster Collection

Related Topics

- Monitoring Systems, Clusters, and Events
- Default Public Collections
- System Status Types
- Software Status Types

Creating System or Cluster Collections

Perform the following procedure to create a new private or shared system or cluster collection.

Note:



Users with full-configuration-rights can create a shared collection. Users who have limited-configuration-rights can only create his or her own private collections. They can, however, view shared collections.

To create a new system or cluster collection:

1. Click **Customize** in the **Systems and Events** panel. The **Customize Collections** page appears.
2. In the **Show** dropdown list, select **Systems**. All available system or cluster collections are displayed.
3. Click **New**. The **New Collection** section appears.
4. Select **Choose members individually** or **Choose members by attributes**.
5. If you selected **Choose members individually**, complete the following:
 - a. In the **Choose from** dropdown list, select an individual collection or collection member.
Note: When a collection is selected from the dropdown list, the first-level members of that collection are displayed in the **Available Items** box.
 - b. From the **Available Items** box, select items to place in the collection by highlighting the item and clicking >>. You can click the up and down arrow to change the position of an item in the collection, or click **Remove** to remove items from the **Selected Items** box.
 - c. Click **Save As** to save the collection. The **Save As** section appears. You can click **Cancel** to close the **New Collection** section without saving changes. Refer to “Saving Collections” for more information on saving a collection.
6. If you selected **Choose members by attributes**, the **New** section appears.
 - a. In the **Search for** dropdown list, select **systems** or **clusters**.
 - b. Enter the search criteria for the collection. Refer to “Performing an Advanced Search for Systems” for more information on system search criteria or “Performing an Advanced Search for Clusters” for more information on cluster search criteria.
 - c. Click **View** to conduct the search immediately or click **Save As** to save the collection. The **Save As** section appears. Refer to “Saving Collections” for more information on saving collections. Or click **Cancel** to close the **New Collection** section without saving changes.

Command Line Interface

Users with full-configuration-rights user can use the **mxcollection** command to create new collections from the command line interface (CLI).

Refer to “Using Command Line Interface Commands” for more information on accessing the manpage, which includes detailed information for this command.

Related Procedures

- Performing an Advanced Search for Systems
- Editing System or Cluster Collections
- Deleting System or Cluster Collections
- Setting Properties for a System or Cluster Collection

Related Topics

- Monitoring Systems, Clusters, and Events
- Customizing System or Cluster Collections
- Navigating the Systems and Events Panel

Editing System or Cluster Collections

Perform the following procedure to edit a system or cluster collection.

Note:



Users with full-configuration-rights can edit a shared collection. Users who have limited-configuration-rights can only edit his or her own private collections. They can, however, view shared collections.

To edit an existing system or cluster collection:

1. Click **Customize** in the **Systems and Events** panel. The **Customize Collections** page appears.
2. In the **Show** dropdown list, select **Systems**. All available system or cluster collections are displayed. Click  to expand all system and cluster collections in the table, or click  to collapse all system and cluster collections in the table.
3. Select the system or cluster collection to edit, and click **Edit**. The **Edit Collection** section appears.
4. Change the system or cluster criteria. Refer to “Performing an Advanced Search for Systems” for more information on system search criteria or “Performing an Advanced Search for Clusters” for more information on cluster search criteria.
5. Click **View** to run the search immediately, click **Save** to save the edits, or click **Cancel** to cancel all changes.

Command Line Interface

Users with full-configuration-rights user can use the `mxcollection` command to edit existing collections from the command line interface (CLI).

Refer to “Using Command Line Interface Commands” for more information on accessing the manpage, which includes detailed information for this command.

Related Procedures

- Performing an Advanced Search for Systems
- Creating System or Cluster Collections
- Deleting System or Cluster Collections
- Setting Properties for a System or Cluster Collection

Related Topics

- Monitoring Systems, Clusters, and Events
- Customizing System or Cluster Collections
- Navigating the Systems and Events Panel

Deleting System or Cluster Collections

Perform the following procedure to delete a system or cluster collection.

Note:



Users with full-configuration-rights can delete a shared collection. Users who have limited-configuration-rights can only delete his or her own private collection. They can, however, view shared collections.

To delete a system or cluster collection:

1. Click **Customize** in the **Systems and Events** panel. The **Customize Collections** page appears.
2. In the **Show** dropdown list, select **Systems**. All available system or cluster collections are displayed. Click  to expand all system and cluster collections in the table, or click  to collapse all system and cluster collections in the table.
3. Select the collection to be deleted.
4. Click **Delete**. A dialog box appears. Click **OK** to continue with the deletion, or click **Cancel** to cancel the operation. If the selected collection is not empty or is in use by a task, an error message appears.

Command Line Interface

Users with full-configuration-rights user can use the `mxcollection` command to delete existing collections from the command line interface (CLI).

Refer to “Using Command Line Interface Commands” for more information on accessing the manpage, which includes detailed information for this command.

Related Procedures

- Performing an Advanced Search for Systems
- Editing System or Cluster Collections
- Creating System or Cluster Collections
- Setting Properties for a System or Cluster Collection

Related Topics

- Monitoring Systems, Clusters, and Events
- Customizing System or Cluster Collections
- Navigating the Systems and Events Panel

Setting Properties for a System or Cluster Collection

Perform the following procedure to set properties for collections. You can select to make the collection visible in the **Systems and Events** panel or to have it hidden, have the system or cluster status displayed or have it hidden, and select the default view for the collection.

To set properties for system or cluster collections:

1. Click **Customize** in the **Systems and Events** panel. The **Customize Collections** page appears.
2. In the **Show** dropdown list, select **Systems**. All available system or cluster collections are displayed. Click  to expand all system and cluster collections in the table, or click  to collapse all system and cluster collections in the table.
3. Select a collection and click **Set Properties**. The **Set Properties** section appears.
4. Under **Visible**, select **Yes, show items in Systems and Events panel**, or select **No, do not show item in Systems and Events panel**. You might want to select **No, do not show item in Systems and Events panel** if you have collections that are unused, so that they do not clutter the **Systems and Events** panel.
5. Under **Status Displayed**, select **Yes, show status in Systems and Events panel** if you prefer to see the system health status, or select **No, do not show the status in Systems and Events panel** to keep the panel uncluttered.

Note: This option is available only for collections defined by their attribute.

Note: For a collection, the most critical status of its members is displayed. If you open the collection, the status for each individual member is shown.

Note: Try to limit the display of status to only those collections you need, because this uses system resources.

6. In the **Default View** field, select the default view from the dropdown list. Select from **TreeView**, **TableView**, or **IconView**. Refer to “Navigating the Systems and Events Panel” for more information on each view.

Command Line Interface

Users with full-configuration-rights user can use the **mxcollection** command to set properties for collections from the command line interface (CLI).

Refer to “Using Command Line Interface Commands” for more information on accessing the manpage, which includes detailed information for this command.

Related Procedures

- Performing an Advanced Search for Systems
- Editing System or Cluster Collections
- Creating System or Cluster Collections
- Deleting System or Cluster Collections

Related Topics

- Monitoring Systems, Clusters, and Events
- Customizing System or Cluster Collections
- Navigating the Systems and Events Panel

Customizing Event Collections

The **Systems and Events** panel contains an **Events** collection. This collection contains collections of different types of events.

Collections can be private or shared. Shared lists are visible to all users, and private collections are personal collections you create that only you can view. HP Systems Insight Manager (HP SIM) ships with several predefined shared collections. For example, Events by Severity is a default public collection that ships with HP SIM. Refer to “Shared Event Collections” for information on default public collections.

- There are two access levels for the event collections: shared and private. All of the default event collections are shared.
- Every valid user can view and edit his or her own event collections.
- Every valid user can view shared collections, but only the user who has full-configuration-rights can modify the content of shared collections. When the modification is done, every valid user can see the changes.
- Clicking an event collection from an **Events** group displays the result of running the selected event collection in the workspace area of the page. Refer to “Navigating the Event Table View Page” for detailed information on event view page.

To customize an event collection, click **Customize** in the **Systems and Events** panel. The **Customize Collections** page appears. In the **Show** dropdown list, select **Events**. All available **Events** are displayed. Click  to expand all event collections in the table, or click  to collapse all event collections in the table.

On the **Customize Collections** page for events, five options are available:

- **New**. Used to create a new event collection. If you have full-configuration-rights, you can save the new collection as a shared event collection. Otherwise, you can only save it as a private collection. Refer to “Performing an Advanced Search for Events” for more information on creating an event collection.
- **Edit**. Used to edit an existing event collection. With full-configuration-rights, you can edit shared event collections. Refer to “Editing Event Collections” for more information.
- **Delete**. Used to delete existing event collections. With full-configuration-rights, you can delete shared event collections. To delete an existing collection, highlight the collection in the table and click **Delete**. A dialog box appears. Click **OK** to continue with the deletion, or click **Cancel** to cancel the deletion. Refer to “Deleting Event Collections” for more information.
- **Set Properties**. Used to set the display status flag, hidden flag, and the default view. Refer to “Setting Properties for an Event Collection” for more information.

Command Line Interface

Users with full-configuration-rights user can use the `mxcollection` command to set properties for collections from the command line interface (CLI).

Refer to “Using Command Line Interface Commands” for more information on accessing the manpage, which includes detailed information for this command.

Related Procedures

- Performing an Advanced Search for Events
- Editing Event Collections
- Creating Event Collections
- Deleting Event Collections
- Setting Properties for an Event Collection

Related Topics

- Monitoring Systems, Clusters, and Events
- Default Public Collections
- Service Notification Events

Creating Event Collections

Perform the following procedures to create a new event collection.

Note:



By default, all newly created collections are private.

Note:



Users with full-configuration-rights can create a new shared event collection. Users with limited or no configuration rights or can only create their own collections. They can, however, view shared collections.

To create a new event collection:

1. Click **Customize** in the **Systems and Events** panel. The **Customize Collections** page appears.
2. In the **Show** dropdown list, select **Events**. All available event collections are displayed.
3. Click **New**. The **New Collection** section appears.
4. Select **Choose members individually** or **Choose members by attributes**.

5. If you selected **Choose members individually**:
 - a. In the **Choose from** dropdown list, select an individual collection or collection member.
Note: When a collection is selected from the dropdown list, the first level members of that collection are displayed in the **Available Items** box.
 - b. From the **Available Items** box, select items to place in the collection by highlighting the item and clicking **>>**. You can click the up and down arrow to change the position of an item in the collection, or click **Remove** to remove items from the **Selected Items** box.
 - c. Click **Save As** to save the collection. The **Save As** section appears. You can click **Cancel** to close the **New Collection** section without saving changes. Refer to “Saving Collections” for more information on saving a collection.

6. If you selected **Choose members by attributes**, the **New** section appears.
 - a. In the **Search for** dropdown list, select **systems** or **clusters**.
 - b. Enter the search criteria for the collection. Refer to “Performing an Advanced Search for Events” for more information on event search criteria.
 - c. Click **View** to conduct the search immediately or click **Save As** to save the collection. The **Save As** section appears. Refer to “Saving Collections” for more information on saving collections. Or click **Cancel** to close the **New Collection** section without saving changes.

Command Line Interface

Users with full-configuration-rights user can use the **mxcollection** command to create new collections from the command line interface (CLI).

Refer to “Using Command Line Interface Commands” for more information on accessing the manpage, which includes detailed information for this command.

Related Procedures

- Performing an Advanced Search for Events
- Editing Event Collections
- Deleting Event Collections
- Setting Properties for an Event Collection

Related Topics

- Monitoring Systems, Clusters, and Events
- Customizing Event Collections
- Navigating the Systems and Events Panel

Editing Event Collections

Perform the following procedure to edit an event collection. The **Event Collections** section enables you to add, delete, and reorder the position of members of an existing collection. This section is very similar to the **New Collection** section.

Note:



Users with full-configuration-rights can edit a shared collection. Users with full-configuration-rights can only edit their own collections.

To edit an existing event collection:

1. Click **Customize** in the **Systems and Events** panel. The **Customize Collections** page appears.
2. In the **Show** dropdown list, select **Events**. All available event collections are displayed. Click  to expand all event collections in the table, or click  to collapse all event collections in the table.
3. Select the event collection to edit, and click **Edit**. The **Edit Collection** section appears.
4. Change the event criteria. Refer to “Performing an Advanced Search for Events” for more information on event search criteria.
5. Click **View** to run the search immediately, click **Save** to save the edits, or click **Cancel** to cancel all changes.

Command Line Interface

Users with full-configuration-rights user can use the `mxcollection` command to edit existing collections from the command line interface (CLI).

Refer to “Using Command Line Interface Commands” for more information on accessing the manpage, which includes detailed information for this command.

Related Procedures

- Performing an Advanced Search for Events
- Creating Event Collections
- Deleting Event Collections
- Setting Properties for an Event Collection

Related Topics

- Monitoring Systems, Clusters, and Events
- Customizing Event Collections
- Navigating the Systems and Events Panel

Deleting Event Collections

Perform the following procedure to delete an event collection.

Note:



Users with full-configuration-rights can delete a shared collection. Users with limited-configuration-rights or no configuration rights can only delete their own private collections. They can, however, view shared collections.

To delete an event collection:

1. Click **Customize** in the **Systems and Events** panel. The **Customize Collections** page appears.
2. In the **Show** dropdown list, select **Events**. All available event collections are displayed. Click  to expand all event collections in the table, or click  to collapse all event collections in the table.
3. Select the collection to be deleted.
4. Click **Delete**. A dialog box appears. Click **OK** to continue with the deletion, or click **Cancel** to cancel the operation. If the selected collection is not empty or is in use by a task, an error message appears.

Command Line Interface

Users with full-configuration-rights user can use the `mxcollection` command to delete existing collections from the command line interface (CLI).

Refer to “Using Command Line Interface Commands” for more information on accessing the manpage, which includes detailed information for this command.

Related Procedures

- Performing an Advanced Search for Events
- Editing Event Collections
- Creating Event Collections
- Setting Properties for an Event Collection

Related Topics

- Monitoring Systems, Clusters, and Events
- Customizing Event Collections
- Navigating the Systems and Events Panel

Setting Properties for an Event Collection

Perform the following procedure to set properties for collections. You can select to make the collection visible in the **Systems and Events** panel or to have it hidden and select the default view.

To set properties for event collections:

1. Click **Customize** in the **Systems and Events** panel. The **Customize Collections** page appears.

2. In the **Show** dropdown list, select **Events**. All available event collections are displayed. Click  to expand all event collections in the table, or click  to collapse all event collections in the table.
3. Select a collection and click **Set Properties**. The **Set Properties** section appears.
4. Under **Visible**, select **Yes, show items in Systems and Events panel**, or select **No, do not show item in Systems and Events panel**. You might want to select **No, do not show item in Systems and Events panel** if you have collections that are unused, so that they do not clutter the **Systems and Events** panel.
5. In the **Default View** field, select the default view from the dropdown list. Select from **TreeView**, **TableView**, or **IconView**. Refer to “Navigating the Systems and Events Panel” for more information on each view.

Command Line Interface

Users with full-configuration-rights user can use the `mxcollection` command to set properties for collections from the command line interface (CLI).

Refer to “Using Command Line Interface Commands” for more information on accessing the manpage, which includes detailed information for this command.

Related Procedures

- Performing an Advanced Search for Events
- Editing Event Collections
- Creating Event Collections
- Deleting Event Collections

Related Topics

- Monitoring Systems, Clusters, and Events
- Customizing Event Collections
- Navigating the Systems and Events Panel

System Table View Page

Users with full-configuration-rights can manage all shared system collections from the system table view page. Users can also manage their own private collections from this page. They can:

- **Save selections.** Refer to “Saving Collections” for more information.
- **Delete systems from the database.** Select the systems to delete, and click **Delete**. A dialog box appears. Click **OK** to delete the systems, or click **Cancel** to cancel the deletion.
- **Print a system collection results.** Click **Print** to print the collection results. Select **File>Print**.
- **Customize the view.** Click **Customize** to customize which columns display and in what order. Refer to “Customizing the System Table View Page” for more information.

Related Procedures

- Saving Collections
- Customizing the System Table View Page
- Deleting Systems from the Database
- Printing a System Collection Report

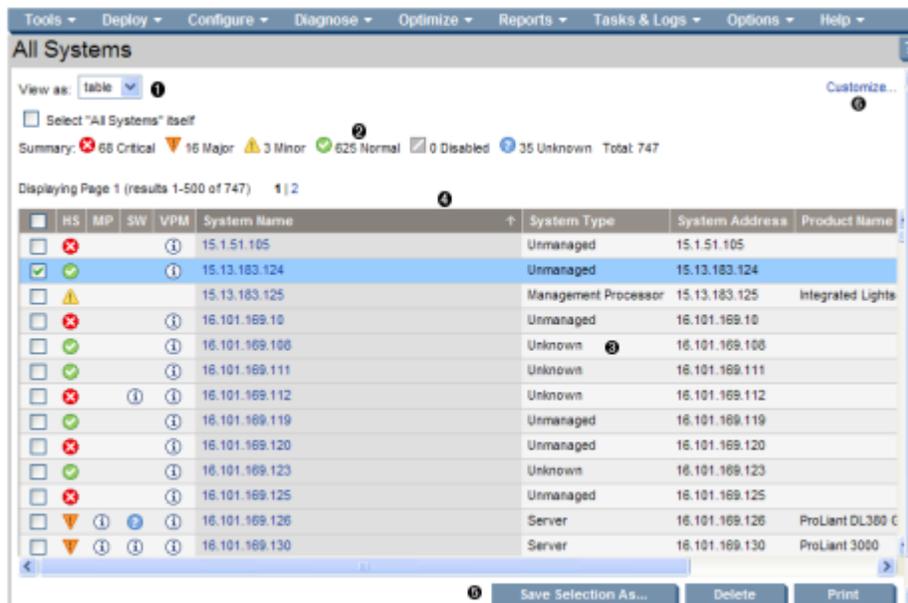
Related Topics

- Navigating the System Table View Page
- Navigating the Picture View Page
- System Status Types
- Software Status Types
- Monitoring Systems, Clusters, and Events

Navigating the System Table View Page

The system table view page is a list of systems that meet common criteria and is divided into the following sections:

1. View Results As
2. System Health Status Legend
3. More System Information
4. System View Columns
5. System Table View Page Buttons
6. Customizing the View



From this page, you can view systems in a list, table, or tree, save system collections, delete systems, and print the system collection.

If a collection results in more than 500 members, the first 500 are displayed on the first page and subsequent pages show the next set of 500 items. Systems selected on one page remain selected

as you navigate to a different page in the collection. Whenever a column is selected as the column to sort by, the entire collection is sorted, not just the items in the currently viewed page.

View Results As

This dropdown list is used to select **table**, which displays the results in a table form, **icons**, which displays only the **HW** status icon and the **System Name** for each system, and **tree** which displays the **HW** status icon and the System Name for each system in a tree format. Refer to “Navigating the Tree View” for more detailed information on the tree view. Refer to “Navigating the Icon View” for more information on the icon view.

System Health Status Legend

The legend shows how many systems in the view are Critical, Major, Minor, Normal, Disabled, and Unknown. Refer to “System Status Types” for more information on system status types.

More System Information

To access a systems view or picture view for a system, click a link in the **System Name** column. Racks link to the rack picture view page, and Enclosures link to the enclosure picture view page. These are both types of container views. Refer to “System Name” for more information.

You can display the system table view page in several ways, including:

- If configured, the **Home** page displays the result of a user-configured collection. By default, this collection is All Servers.
- From the **Systems and Events** panel, click **System Overview**, then click any numbered link.
- From the **Systems and Events** panel, click **Systems**, and then click an existing collection.

After a collection is selected, the results indicate the system name, software status, hardware status, system type, IP address, product model, and columns corresponding to any criteria referenced in the collection. For example, if you include memory condition, the system table view page contains the **Memory** column.

System View Columns

Sort columns by clicking the column header for ascending or descending order. Place your cursor over a column name for a brief description of the column. The columns are not available when you select the **icons** view. Refer to:

- Selection
- System Name
- Health Status
- Management Processor
- Software Status
- HP ProLiant Essentials Performance Management Pack
- HP ProLiant Essentials Vulnerability and Patch Management Pack
- HP ProLiant Essentials Virtual Machine Management Pack
- System Type
- Operating System Name
- System Address
- Product Name

Refer to “Customizing the System Table View Page” for more information on customizing columns.

Selection

Select the checkbox in this column to select a system. You can select more than one system. This option is available in the table view, tree view, and icon view. Select the checkbox in the column heading to select or deselect all displayed systems.

System Name

This column contains the actual system name of all discovered systems. Systems can be shown as a single system or as a system in a container. When you place the cursor over the system name, the full system Domain Name Service (DNS) name is shown, which helps differentiate between two or more systems that share the same system name. If you click the system name link, the **System Page** appears. Refer to “System Page” for more information. If you click a system that is a container (rack or enclosure), the picture view for that object displays. Refer to “Navigating the Picture View Page” for more information.

The **System Name** column displays systems along with their associated devices. The following list shows the associations available in HP Systems Insight Manager (HP SIM):

- Management processor to server
- Server to enclosure
- Management processor to enclosure
- Enclosure to rack
- Switch to enclosure
- System to cluster

The following system types are containers:

- Rack
- Enclosure
- Cluster

When servers and management processors in racks and enclosures are discovered and identified, associations are made between the systems and the racks and enclosures in which they reside. This association displays in the **System Name** column on the system table view page by showing *name* in *system type container name*.

Clicking an enclosure name in the **System Name** column produces a list of all discovered systems in the selected enclosure. The status for both racks and enclosures is always Unknown.

When switches in blade enclosures are discovered and identified, associations are made between the switches and the enclosures in which they reside. This association appears in the **System Name** column on the system table view page by showing *switch_name* in *Encl. enclosure_name*. The **System Type** column displays Switch as the system type. For HP SIM to identify and manage the HP ProLiant p-Class server blades correctly, the HP Insight Management Agent 5.50 or later must be installed on the blades to make associations work and event correlation function properly.

When a server blade is identified through another system in the same rack or enclosure, associations are made between the iLO and the enclosures in which they reside. This association appears in the **System Name** column on the system table view page by showing the system serial number prepended with *Server_* in *Encl. enclosure_name*. For example, *Server_C349KJP5D876* in *Encl. Encl4*. The system address, product name, and operating system are not displayed for these systems.

To launch HP Serviceguard Manager to manage the server belonging to an HP Serviceguard cluster, be sure that:

- HP Serviceguard Manager is installed and registered with HP SIM
- The system selected is an HP-UX or Linux server that belongs to an HP Serviceguard cluster

Health Status

The health status column (indicated by HS) displays the overall system health status, which is determined by the default Hardware Status Polling task. By clicking the status icon in this column, the **HP Management Agents** or the **HP Instant Tootools for Servers** page displays. If the system does not have Web Agents or Instant Tootools installed, the **System Page** displays. Refer to “System Status Types” for more information.

The hardware status displayed for container systems, such as Serviceguard or a complex, it is the actual hardware status for the container itself. For clusters, it is the ping status.

Management Processor

The management processor column (indicated by MP) displays the status icon of the management processor, if the system has an Integrated Lights-Out Board (iLO) installed. Otherwise, the Informational icon is displayed. Clicking on the status icon displays the management processor login page.

Software Status

The software status column (indicated by SW), available for servers only, indicates both the availability of software updates and how critical they are. Refer to “Software Status Types” for more information on the software status types.

If you click an Unknown status, HP SIM displays the **Legacy Version Control** page.

If HP Version Control Agent is installed on the system, clicking the software status icon for that system displays **HP Version Control Agent Software Inventory** page. If you hover your cursor over the status icon and the VCA is not installed on the system, a message appears that states *Version Control Agent not found*.

HP ProLiant Essentials Performance Management Pack

The HP ProLiant Essentials Performance Management Pack (PMP) status column (indicated by PF) displays the cumulative performance status of all monitored subsystems for the system. By clicking the status icon in this column, the **HP ProLiant Essentials Performance Management Pack** page for the selected system displays, providing more detailed performance information.

Note:



If the PMP is not installed on the HP SIM system, this column does not display on the system table view page.

If the PMP is not monitoring a server, the status is Unknown. If you click the status link, the PMP displays a page with information about purchasing a license to monitor that system or shows notification that PMP monitoring is not supported on that system.

Note:



For the **PF** column, a status appears for all systems from the All Servers list. If the status cannot be determined for some reason, the status is set to Unknown.

HP ProLiant Essentials Vulnerability and Patch Management Pack

Vulnerability and Patch Management Pack vulnerability information is displayed in the **VPM** column of the HP SIM console. Initially, the icon depicted in the column displays Vulnerability and Patch Management Pack eligibility information for the target system in the specific row. After target servers are licensed and a vulnerability scan is performed, the column displays the combined status of the last vulnerability scan on the target system (patch status is not displayed in the column). Click the icon to display detailed information about the system status with regard to Vulnerability and Patch Management Pack. Clicking the Normal, Minor, or Major icons opens a new informational page where the last scan results for the system can be accessed. A new scan can also be launched from this page. Clicking the Unknown icon for a system displays an explanatory page listing possible reasons why Vulnerability and Patch Management Pack.

Note:



If Vulnerability and Patch Management Pack is not installed on the HP SIM system, the Informational icon appears in the **VPM** column on the system table view page. Clicking this icon displays information on how to install Vulnerability and Patch Management Pack and purchase licenses.

If the system is not licensed or has not yet been scanned by Vulnerability and Patch Management Pack, the Informational icon appears in the **VPM** column. Clicking this icon displays details about licensing the target system and a link to the HP SIM License Manager or information about vulnerability scanning and a link to scan for or patch vulnerabilities on the target system.

HP ProLiant Essentials Virtual Machine Management Pack

HP ProLiant Essentials Virtual Machine Management Pack (VMM) status column (indicated by **VM Status**) displays the cumulative status of all Virtual Machine Hosts and Virtual Machine Guests. Clicking the status icon on the **VM Status** column displays the **HP ProLiant Essentials Virtual**

Machine Management Pack page for the selected system, providing more information on the status of the Virtual Machine.

Note:



When VMM is not installed on the HP SIM system, this column does not appear on the All Systems system table view page. Similarly, if HP ProLiant Essentials Virtual Machine Management Pack is uninstalled, the **VM Status** is no longer updated in the HP SIM console.

For systems with type as Server and subtype as Virtual Machine Host or Virtual Machine Guest, HP SIM populates the **VM Status** column with appropriate status icons. Refer to “VM Status Types” for more information.

System Type

This column displays the system type, for example, Server, or Desktop. The system type Unmanaged indicates systems that have no management protocol that HP SIM could detect, for example, no Simple Network Management Protocol (SNMP), Web-Based Enterprise Management (WBEM), Desktop Management Interface (DMI), or Secure Shell (SSH). The system type Unknown indicates systems that have some management protocol but have not matched any identification rule in HP SIM. Refer to “System Types” for more information on the different system types.

Note:



Unmanaged systems might indicate that the credentials were not set correctly in order to communicate with the system. If you know that there are HP Insight Management Agents installed, verify the credentials used.

Operating System Name

The operating system column (indicated by OS Name) displays the operating system on the system. For a Serviceguard cluster, this column displays **HP Serviceguard** if the cluster is of type HP-UX or **HP Serviceguard for Linux** if the cluster is of type Linux. **HP Serviceguard** and **HP Serviceguard for Linux** under the **OS Name** column of the *virtual* cluster system column do not represent the actual operating system name and type. This field is used to let you know the servers that make up the cluster are of HP-UX or Linux type, respectively.

System Address

This column displays the primary IP addresses of the system that HP SIM uses to communicate with the system. Not all systems have an IP address, including HP Serviceguard clusters.

Product Name

This column displays the product name of the system.

System Table View Page Buttons

Three buttons at the bottom of the system table view page are available to users with full-configuration-rights. These buttons are not available when using a tool and selecting an individual target system.

- **Save selection as.** When a system is highlighted, this button is used to save the selection with a new name. Changes are saved on a per-user, per-collection basis. Refer to “Saving Collections” for more information.
- **Delete.** This button is used to delete one or more systems from the database. Select the systems to be deleted, and click **Delete**. A dialog box appears. Click **OK** to continue with the deletion or click **Cancel** to cancel the operation. Refer to “Deleting Systems from the Database” for more information.

Note:



If a VM Host is deleted, it can still be accessed through the VMM console, and the operations that can be performed on a VM Host are not affected by the fact that the HP SIM system has been deleted. The VMM console continues to show the HP SIM status.

- **Print.** When the report is displayed, select **File->Print** from the browser menu to print the report.

Note:

Because certain print options are not supported in HP SIM, you cannot:

- Change the **Orientation** to **Landscape** in the **Print** dialog box (refer to **Printing Problems** in “Troubleshooting” for a workaround to this issue)
- Cancel printing after the print job has been executed, but you can access the operating systems print queue and cancel the print job
- Print to a file
- Print selected systems, only entire list of systems
- Print the system table view page if you close the browser immediately after issuing a print request



Buttons are disabled if you do not have appropriate rights. However, the **Print** button appears for all users.

Customizing the View

The **Customize** link is in the upper right corner of the system table view page. Click this link to determine which columns are displayed and in what order. Refer to “Customizing the System Table View Page” for more information.

Related Procedures

- Customizing the System Table View Page
- Saving Collections
- Deleting Systems from the Database
- Printing a System Collection Report

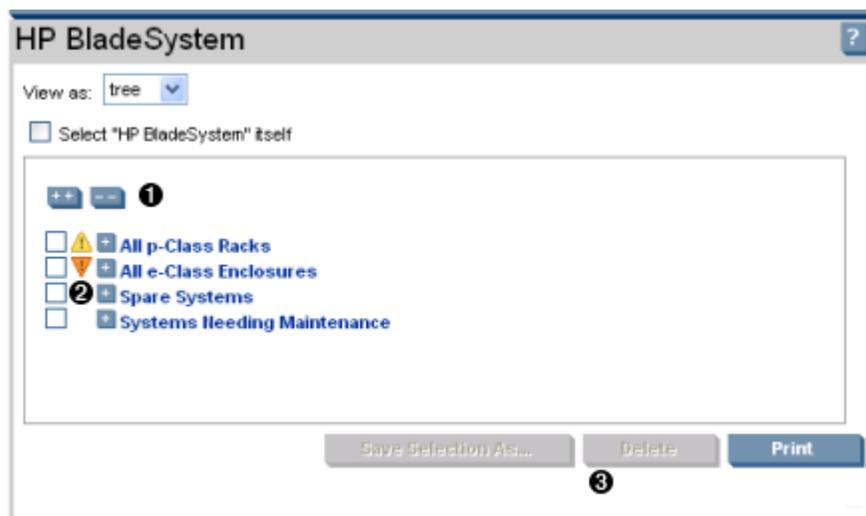
Related Topics

- Monitoring Systems, Clusters, and Events
- System Table View Page
- System Status Types
- Software Status Types
- Navigating the Picture View Page

Navigating the Tree View

When a collection is selected in the **Systems and Events** panel or from the system table view page or event table view page, the tree view is displayed in the workspace. The tree view is initially collapsed. Systems might appear in multiple locations, since they can be in multiple containers. Users are only able to view systems that they are authorized to see. Therefore, if a user is not authorized to view a particular system in the tree, that branch is not displayed. The following sections are available on the tree view page:

1. Expanding the Tree View
2. Tree View Status
3. Tree View Buttons



Expanding the Tree View

Branch nodes can be expanded by clicking the toggling expansion icon. However, the system name is not an expansion control, but a drilldown. When a branch is collapsed, the icon appears as . When clicked, the branch expands to show the child systems, and the icon toggles to . Clicking the icon again collapses the branch and toggles the icon back.

Note:



The expansion state persists only for the page session. When the page is reloaded or navigated to again, a fresh tree is loaded. This is to ensure that all newly discovered systems are added to the view.

Note:



The tree branch expansions differ from the **Systems and Events** panel and the workspace. In the **Systems and Events** panel, the branch can be expanded by clicking the icons or the branch label. In the workspace, the branch can be expanded by clicking the icon only, since clicking the system name invokes the drilldown feature.

A paging mechanism is provided in the branches. When a branch is expanded, the first 100 systems are displayed. To view additional systems, click **next...of...**. Clicking this link displays the remaining systems, up to 100. If only one system remains in the next page, it is simply added to the page in place of the **next** link.

At the top of each tree view there are two expansion buttons. To expand all branches of the tree, click . To collapse all branches of the tree to first level branches, click . If there are too many systems to load into the expand all page, a popup message appears stating that there are too many systems in the tree and the function cannot be performed.

Selection in the Tree View

The selection control for the tree view cycles through four states using the following check icons:



First, initial state, nothing selected.



Second state, both the container and the contents are selected. If the contents were not already expanded, the next level of children are expanded to show the selection.



Third state, all of the contents are recursively selected. The children are expanded (if not already) to show they are selected. Only the next level is expanded.



Fourth state, just the container is selected.

Tree View Status

The tree view displays status data for each system. The status icon is located in the left of the tree view next to the selection checkbox. If the status of the systems is Unknown, no status icon appears. If the systems are containers, the status to the left of the container name is shown as the most critical status of the systems in the container, including the container status. The status of the container itself is displayed to the right of the system name along with a system type label.

Available Drilldowns

The tree view contains hyperlinks for the system name and status icon drilldowns. If a system name is clicked, the **System Page** for that particular system appears. The status icons drilldown to the status URL for that system, unless the status icon is the status icon to the left of a container. Clicking on the roll-up status of a branch loads a table view of all the systems in that branch which match the roll-up status. Thus, you are presented with all the systems that are contributing to the severity of the roll-up status.

Selection States for Collections

In the tree view, you cannot select a collection and the members of the same collection simultaneously. When a collection is selected, the members are displayed, and their selection boxes are disabled. The selection states for a collection are:



The initial state, nothing is selected



The collection itself is selected and the contents of the collection are disabled



The members of collection are selected; the collection itself is unselected

Additionally, there is a checkbox at the top of the tree that enables you to select the collection that is being viewed. When the checkbox is checked, all the checkboxes under the collection are cleared and disabled. When the checkbox is deselected, the checkboxes under the collection become selectable.

Tree View Buttons

Three buttons at the bottom of the tree view page are available to users with full-configuration-rights.

- **Save selection as.** When a system or group of systems is selected, this button is used to save the selection with a new name. Changes are saved on a per-user. Refer to “Saving Collections” for more information.

- **Delete.** This button is used to delete one or more systems from the database. Select the systems to be deleted, and click **Delete**. A dialog box appears. Click **OK** to continue with the deletion or click **Cancel** to cancel the operation. The tree view is refreshed. Refer to “Deleting Systems from the Database” for more information.

Note:



Only systems can be deleted from the tree view. If a collection is selected, the **Delete** button becomes disabled. Collections must be deleted through the **Customize Collections** page. Refer to “Deleting System or Cluster Collections” for more information on deleting collections.

Note:



If a VM Host is deleted, it can still be accessed through the VMM console, and the operations that can be performed on a VM Host are not affected by the fact that the HP Systems Insight Manager (HP SIM) system has been deleted. The VMM console continues to show the HP SIM status.

Note:



If you select a collection by checking **Select "collection name" collection** itself, the **Delete** button is disabled. To delete collections, go to the **Customize Collections** page. Refer to “Deleting System or Cluster Collections” or “Deleting Event Collections” for more information.

- **Print.** Click **Print** to display a printable version of the tree. To print the tree, from the browser, select **File>Print**.

Buttons are disabled if you do not have appropriate rights. However, the **Print** button appears for all users.

Related Topics

- Navigating the System Table View Page
- Navigating the Event Table View Page
- Navigating the Picture View Page

Navigating the Icon View

The icon view lists the system name of all discovered systems as well as the System Health Status for each system. The legend shows how many systems in the view are Critical, Major, Minor, Normal, Disabled, and Unknown. Select the checkbox next to system name to select a system. You can select more than one system or to select all an entire collection, select the checkbox, **Select "collection name" itself**. This page includes the following sections:

1. View Results As

2. System Health Status Legend
3. Icon View Buttons

The screenshot shows the 'Systems by Type' interface. At the top, there is a 'View as' dropdown menu set to 'icons'. Below it is a checkbox labeled 'Select "Systems by Type" itself'. A summary bar displays the following status counts: 0 Critical (red circle with exclamation mark), 6 Major (orange triangle), 1 Minor (yellow triangle), 65 Normal (green circle), 0 Disabled (grey square), 0 Unknown (blue circle), and Total: 72. The main area is a table of systems, each with a status icon (green circle for Normal, orange triangle for Major, yellow triangle for Minor, red circle for Critical, grey square for Disabled, blue circle for Unknown) and a system name. At the bottom of the table, there are three buttons: 'Save Selection As...', 'Delete', and 'Print'.

View Results As

This dropdown list is used to select **table**, which displays the results in a table form, **icons**, which displays only the **HW** status icon and the **System Name** for each system, and **tree** which displays the **HW** status icon and the System Name for each system in a tree format. Refer to “Navigating the Tree View” for more detailed information on the tree view. Refer to “Navigating the System Table View Page” for more information on the system table view.

System Health Status Legend

The legend shows how many systems in the view are Critical, Major, Minor, Normal, Disabled, and Unknown. Refer to “System Status Types” for more information on system status types.

Icon View Buttons

Three buttons at the bottom of the icon view page are available to users with full-configuration-rights.

- **Save selection as.** When a system or group of systems is selected, this button is used to save the selection with a new name. Changes are saved on a per-user basis. Refer to “Saving Collections” for more information.
- **Delete.** This button is used to delete one or more systems from the database. Select the systems to be deleted, and click **Delete**. A dialog box appears. Click **OK** to continue with the deletion or click **Cancel** to cancel the operation. The icon view is refreshed. Refer to “Deleting Systems from the Database” for more information.

Note:



If a VM Host is deleted, it can still be accessed through the VMM console, and the operations that can be performed on a VM Host are not affected by

the fact that the HP Systems Insight Manager (HP SIM) system has been deleted. The VMM console continues to show the HP SIM status.

Note:



If you select a collection by checking **Select "collection name" collection** itself, the **Delete** button is disabled. To delete collections, go to the **Customize Collections** page. Refer to “Deleting System or Cluster Collections” or “Deleting Event Collections” for more information.

- **Print.** Click **Print** to display a printable version of the tree. To print the icon view, from the browser, select **File->Print**.

Related Topics

- Navigating the System Table View Page
- Navigating the Tree View
- Navigating the Picture View Page

Navigating the Picture View Page

The **Picture View** page appears when a container is selected from the **System Name** column on the system table view page. The container view page displayed depends on the type of container selected. For example, if a rack is selected, the **Rack View** page appears. The following are the types of container collection views:

- Rack View Page
- Enclosure View Page

Rack View Page

The picture view page for racks and enclosures contains a diagram of the discovered systems in the rack or enclosure if available. The rack name appears along with a picture view, table view, or iconic view of the rack. While signed in to HP Systems Insight Manager (HP SIM), placing your cursor over a server shown in the view, displays information on that particular server, including server blade name, slot number, and the enclosure in which the server is located. You can also click a server name to display information about the server. The **System Page** appears.

Enclosure View Page

The picture view page for enclosures contains a diagram of the discovered systems in the enclosure if available. The enclosure name appears along with a picture view, table view, or iconic view of the enclosure. While signed in to HP SIM, placing your cursor over a server shown in the view, displays information on that particular server, including server blade name, slot number, and the enclosure in which the server is located. You can also click a server name to display information about the server. The **System Page** appears.

The following systems are displayed in the picture view for racks and enclosures:

- Servers of desktops

- Interconnect switch
- Power supply enclosure

Also displayed in the picture view for enclosures are slots that have no server or desktop identified and no interconnect switch identified.

Customizing the View

You can change the way the picture view page appears. Click the down arrow on the **View as** dropdown list, and select **table**, **icon**, or **picture view**. However, the picture view is only available if you have already drilled down to a rack or enclosure by clicking the rack or enclosure name on the system table view page and *then* switched back to a tabular or iconic view. Drilling down into a rack or enclosure restricts the systems to only those that pertain to the rack or enclosure. It is then possible to switch back and forth between the other view types.

Related Topics

- System Table View Page
- Navigating the System Table View Page

About Management Processors

HP Systems Insight Manager (HP SIM) uses HTTP and SNMP for identifying management processors. Previous versions of HP SIM used only SNMP identification to identify management processors and obtain their statuses. Now, HTTP identification is performed first, followed by SNMP identification. If a new management processor has been installed in the server, the Web agents must be reinstalled on the server, or the management processor might not be correctly identified. If both the server and the management processor have been discovered and identified, an association is made. The association between the management processor and the server displays in the **System Name** column on the system table view page by showing "*management processor*" in server "*system*."

SNMP Status Polling obtains the status for the host server. HP SIM can distinguish between the following management processor products:

- Remote Insight Board PCI
- Remote Insight Board EISA
- Remote Insight Lights-Out Edition (RILOE)

The system table view page provides information about management processors:

- The server entry displays a **Status** icon in the **MP** column. The tool tip for the icon displays the status of the management processor. Clicking this icon launches the **Remote Insight Home** page.
- The management processor entry displays the name of the server with which the management processor is associated by showing "*management processor*" in server "*system*."
- For all remote management processor entries, the **System Type** field states **management processor**, and the **Product Name** field states **Remote Insight Management**.

The system table view page contains an **MP** column, which displays the status of the management processor. There are seven different status levels (Critical, Major, Minor, Normal, Warning,

Disabled, and Unknown). These status level icons are the same status level icons used for software status. Refer to “Software Status Types” for more information on each status type.

The management processor status icons launch the **Remote Insight Home** page and display in a separate browser. On this page, you can find the following information:

- Current User
- Server Name
- Server Power Status
- Remote Insight IP Address
- Remote Insight Name
- Latest Integrated Management Log Entry
- Latest Remote Insight Event Log Entry
- Remote Insight Mouse Cable

Clicking the management processor in the **System Name** column launches the **System Page** for that management processor. Refer to “Identity Tab for Servers” for more information.

For a server with a Remote Insight board, the **System Page** includes the **Management Processor Information** box.

Related Topics

- System Table View Page
- Navigating the System Table View Page
- Navigating the Picture View Page
- System Page
- System Types

About Racks and Enclosures

HP Systems Insight Manager (HP SIM) discovers and identifies server blade racks and enclosures.

There are two specific search criteria for racks and enclosures:

- Rack
- Enclosure

Running searches using these criteria returns a list of systems contained in the selected racks or enclosures. Any criteria, except for the two listed previously, returns the racks and enclosures themselves, not the systems in those racks and enclosures. For instance, a **system name** search for the rack **Franklin 1** would return the system **Franklin 1**, not any systems *in* **Franklin 1**.

Two default collections are related to racks and enclosures and are listed under the **System Type** collection:

- All Racks

- All Enclosures

On the system table view page, racks display in two formats:

- Encl1 in Rack1
- Rack1

The **Picture View** page can be displayed by clicking rack hyperlink.

Clicking an enclosure name in the **System Name** column on the system table view page produces a list of all discovered systems in the selected enclosure. The status for both racks and enclosures is always Unknown.

The **Picture View** page displays if the server is part of an enclosure or rack. This page contains a diagram of the discovered systems in the enclosure and, if available, in the rack. While signed into HP SIM and placing your cursor over a server shown in the view, you receive information on that particular server, including server blade name, slot number, and the enclosure in which the server is located.

Related Topics

- System Table View Page
- Navigating the System Table View Page
- Navigating the Picture View Page

Customizing the System Table View Page

Perform the following procedure to customize the system table view page by selecting the columns to be displayed and the sort order.

To customize the system table view page:

1. On the system table view page, click **Customize**. The **Customize Table Appearance** page appears.
2. Select the columns you want displayed in the **Available Columns** box, and click >> to add the columns to the **Displayed Columns** box.
3. To remove one or more columns from the display, select the columns in the **Displayed Columns** box, and click << to move them to the **Available Columns** box.
4. To sort the collection results by a particular column, select a column from the **Sort by** dropdown list.
5. Select **Ascending** or **Descending**.
6. To apply the customization to all system collections, select **Apply to all system collections**.
7. Click **OK** to save selections and return to the system table view page, or click **Cancel** to cancel all changes and return to the system table view page.

Related Procedures

- Saving Collections

- Deleting Systems from the Database
- Printing a System Collection Report

Related Topics

- System Table View Page
- Navigating the System Table View Page

Deleting Systems from the Database

Perform the following procedure to delete one or more systems from the HP Systems Insight Manager (HP SIM) database.

Note:



Deleting many systems at one time, from the database, results in a performance delay.

Note:



The central management server (CMS) cannot be deleted.

Note:



Clusters that contain cluster members cannot be deleted. To delete a cluster with its cluster members, you must first go to the system table view page by selecting the **All Systems** collection in the **Systems and Events** panel. Then, select the cluster along with all of its members and click **Delete**.

To delete systems:

1. On the system table view page, select one or more systems to delete from the HP SIM database by selecting them in the results display.
2. Click **Delete**. A dialog box appears stating *Are you sure you want to delete these systems?*
3. Click **OK** to delete the systems, or click **Cancel** to return to the system table view page without deleting the events.

Note:



Containers (for example, racks) must be empty before they can be deleted. Selecting a rack and all its contained systems works without error.

Note:



Some systems that host management proxies (such as the WMI Mapper Proxy or an SMI-S provider) cannot be removed until all dependant systems are also removed.

Related Procedures

- Saving Collections
- Printing a System Collection Report
- Customizing the System Table View Page

Related Topics

- System Table View Page
- Navigating the System Table View Page

Printing a System Collection Report

Perform the following procedure to print the system collection results.

To view and print system collection results reports:

1. On the system table view page, click **Print**.
A printable window appears
2. Click **Print** to print the report.
3. When the report is displayed, select **File->Print** from the browser menu to print the report.

Because the following print options are not supported in HP Systems Insight Manager (HP SIM), you cannot:

- Change the **Orientation** to **Landscape** in the **Print** dialog box, refer to “Printing” for a workaround to this issue
- Cancel printing after the print job has been executed, but you can access the operating systems print queue and cancel the print job
- Cancel printing to a file
- Print selected systems, not entire list of systems

- Print the system table view page if you close the browser immediately after issuing a print request

Related Procedures

- Saving Collections
- Deleting Systems from the Database
- Customizing the System Table View Page

Related Topics

- System Table View Page
- Navigating the System Table View Page

System Status Types

In HP Systems Insight Manager (HP SIM), a system has one of the following health status types:

Status Icon	Icon Meaning	Description
	Critical	HP SIM can no longer communicate with the system. The system was previously discovered but cannot be pinged. The system might be down, powered off, or no longer accessible on the network because of network problems.
	Major	A major problem exists with this system, it should be addressed immediately. For systems running HP Insight Management Agent, some component has failed. The system might no longer be properly functioning, and data loss can occur. In Insight Manager (WIN32), this status was identified as <i>Failed</i> .
	Minor	A minor problem exists with this system. For systems running Insight Management Agent, some component has failed but the system is still functioning. In Insight Manager (WIN32), this status was identified as <i>Degraded</i> .
	Warning	The system has a potential problem or in a state that might become a problem.
	Normal	The system is operating normally. The system is accessible.

Status Icon	Icon Meaning	Description
	Disabled	The system is suspended. This enables a system to be excluded from status polling, identification, data collection, and automatic event handling. On the Automatic Discovery page, if you select the option Automatically discover a server blade when its iLO is identified , new servers discovered through Integrated Lights Out (iLO) (for example, no operating system or IP address known) are shown as disabled, until the system is discovered with an IP address or operating system.
	Unknown	HP SIM is not able to obtain management information about the system using SNMP or DMI. Although no management instrumentation information is available, the system can be pinged. It might have an invalid community string or security setting, or it might be an IP address that is no longer associated with a system.
	No Status	The system has not been polled by one or more of the polling tasks since the system was discovered.
	Informational	The system might be in a transitional state or a non-error state.

Note:



HP Insight Management Agent for Servers for Windows continue to use the terms Normal, Degraded, Failed, and Inaccessible. Minor and Major status are only associated with systems running these agents.

Related Topic

- [System Table View Page](#)

WBEM Operational Status Types

HP Systems Insight Manager (HP SIM) reports WBEM operational status for storage and server elements, such as storage switch ports and filled memory slots. The following statuses are available:

Status Icon	Icon Meaning	Description
	Non-recoverable error, Lost communication	<p>HP SIM can no longer communicate with the element.</p> <ul style="list-style-type: none"> ● Non-recoverable indicates that the element has failed and recovery is not possible. ● Lost communication indicates that the element was previously discovered, but is currently unreachable.
	Predictive Failure, Error, Aborted, Supporting Entity in Error	<p>A major problem exists with this system and should be addressed immediately.</p> <ul style="list-style-type: none"> ● Predictive Failure indicates that the element is functioning nominally, but a failure is likely to occur in the near future. ● Error indicates that the element is in an error state. ● Aborted indicates that the element's functionality has stopped abruptly. The element's configuration might need to be updated. ● Supporting Entity in Error indicates that the element may be functioning normally, but an element it depends on is in an error state.

Status Icon	Icon Meaning	Description
	Degraded, Stressed	<p>A minor problem exists with this element.</p> <ul style="list-style-type: none"> ● Degraded indicates that the element is not operating at optimal performance or might be reporting recoverable errors. ● Stressed indicates that the element is functioning, but needs attention.
	OK	The element is operating normally.
	In service, Stopped	<p>The element is suspended.</p> <ul style="list-style-type: none"> ● In Service indicates that the element is being configured. ● Stopped indicates that element is stopped.
	Unknown, No contact	<p>No management information about the element could be obtained.</p> <ul style="list-style-type: none"> ● Unknown indicates that the element status is not available. ● No Contact indicates that the element exists, but HP SIM has never been able to communicate with it.

Status Icon	Icon Meaning	Description
	Starting, Stopping, Dormant, Power Mode, Other	<p>This status provides useful information about the port. No attention is required.</p> <ul style="list-style-type: none"> ● Starting indicates that the element is starting. ● Stopping indicates that element is stopping. ● Dormant indicates that the element is inactive. ● Other indicates that additional information is available, but it does not fit into the previously listed categories.

Related Topics

- Identity Tab for a Tape Library
- Identity Tab for a Storage Switch

Software Status Types

In HP Systems Insight Manager (HP SIM), system software has one of the following status types:

Status Icon	Icon Meaning	Description
	Major	An update that contains a critical bug fix is available for this system.
	Minor	An update that contains new hardware support or bug fixes is available for this system.
	Normal	All components on the system match the repository.
	Disabled	The system is suspended; therefore, no software status is available.
	Informational	The central management server (CMS) could not reach the HP Version Control Agent on the system, so the status of the system is unknown.
	Unknown	HP Version Control Agent (VCA) cannot communicate with HP Version Control Repository Manager (VCRM).

Note:

The Unknown status appears for server systems only and under any of the following circumstances:



- The VCA is not installed on the managed server.
- The VCA is installed on a server, but that server does not have a trust relationship established with HP SIM.
- The operating system on the target server is not supported. Windows and Linux operating systems are supported.
- The correct version of the agent is not on the target system.
- The target server type brand is not supported (only HP or Compaq brand servers are supported).
- The target system is not licensed for monitoring by the HP ProLiant Essentials Performance Management Pack (PMP). The target system must have the HP Insight Management Agent 6.20 or later installed.
- PMP reports an indeterminate status for the system.

Related Topic

- [System Table View Page](#)

Cluster Table View Page

To access Cluster collections, click **Systems** in the **Systems and Events** panel. Users with full-configuration-rights can manage all shared cluster collections from the cluster collection view. Users can manage their own private collections from this page as well. They can:

- **Save collections.** Click **Save Selection as** from the cluster table view page.
- **Delete clusters.** Click **Delete** from the cluster table view page. A confirmation box is displayed. Click **OK** to delete the cluster, or click **Cancel** to cancel the deletion.

Note:



Clusters that contain cluster members cannot be deleted. To delete a cluster with its cluster members, you must first go to the system table view page by selecting the **All Systems** collection in the **Systems and Events** panel. Then, select the cluster along with all of its members and click **Delete**.

-
- **Print cluster collection results.** Click **Print** to print the collection results.

- **Customize the view.** Click **Customize** to customize which columns display and in what order. Refer to “Customizing the Cluster Table View Page” for more information.

Related Procedures

- Customizing the Cluster Table View Page
- Deleting Clusters from the Database
- Printing a Cluster Collection Report
- Saving Collections

Related Topic

- Cluster Monitor

Navigating the Cluster Table View Page

A cluster collection logically groups clusters into a collection based on information in the HP Systems Insight Manager (HP SIM) database. Creating logical groups of clusters reduces the number of clusters viewed in a particular cluster collection. Cluster Monitor can be launched from the cluster table view page in two ways:

- Clicking the name of the cluster in the **Cluster Name** column
- Clicking the cluster status icon in the **CS** column

Note:



Cluster Monitor is an MSCS only tool which shows information (such as the groups, resources and so on of an MSCS cluster) for that cluster. For all other clusters, excluding HP Serviceguard clusters, clicking the name of the cluster in the **Cluster Name** column or cluster status icon in the **CS** column brings up the **System Page** for that cluster. Refer to “Cluster Name” and “CS” for more information.

Complex collections that contain individual member selections or numerous search criteria take more system resources to run. Keep the collection as simple as possible to minimize performance impacts of individual tasks.

Note:



Not all users can view all clusters. The results of the collection depend on the clusters that were assigned to the user who initiated the collection. Each user is only able to view the clusters that are assigned to them by a user with full-configuration-rights. A user with full-configuration-rights assigns managed clusters using user authorizations.

The cluster table view page is divided into the following sections:

1. View As
2. Cluster Status Legend
3. Customizing the View

4. Cluster Collection Columns
5. Buttons

Refer to “Creating New Authorizations” for more information.

The screenshot shows the 'All Clusters' page with a table view. The table columns are: Cluster Name, Cluster Address, Cluster Type, and Cluster Description. The 'atw' cluster is selected. A summary bar at the top indicates: 1 Critical, 3 Major, 0 Minor, 4 Normal, 0 Disabled, 29 Unknown, Total: 37.

Cluster Name	Cluster Address	Cluster Type	Cluster Description
ACSL-Support-Metro		HP Serviceguard	HP Serviceguard Cluste...
atw	16.140.160.106		
autos_cluster		HP Serviceguard	HP Serviceguard Cluste...
BASIC_movie_200506060525		HP Serviceguard	HP Serviceguard Cluste...
benado	16.129.66.23	OVMS	OpenVMS Cluster system
COE-8		HP Serviceguard	HP Serviceguard Cluste...
cluster_choice		HP Serviceguard	HP Serviceguard Cluste...
cluster1		HP Serviceguard	HP Serviceguard Cluste...
guru	16.140.160.14	TruCluster	HP TruCluster Server
INFREQUENT_dawn_200506030728		HP Serviceguard	HP Serviceguard Cluste...
INFREQUENT_dawn_200506091038		HP Serviceguard	HP Serviceguard Cluste...
INFREQUENT_movie_200506010727		HP Serviceguard	HP Serviceguard Cluste...
INFREQUENT_spare_200506081740		HP Serviceguard	HP Serviceguard Cluste...
jyeshh_ascii		HP Serviceguard	HP Serviceguard Cluste...
jyeshh_pina_split		HP Serviceguard	HP Serviceguard Cluste...

From this page, you can save the collection with a new name, delete one or more clusters from the collection, customize the collection, and print the cluster collection report. In a multi-user environment, only one user at a time can edit a collection. If another user wants to edit the same collection, a **List Edit Warning** box appears. The user can cancel the editing request or edit the collection and save it as a new collection.

View As

This dropdown list is used to select **table**, which displays the results in a table form, or **tree**, which displays all of the clusters in the collection in a tree form. Refer to “Navigating the Tree View” for more information on navigating the tree view.

Cluster Status Legend

The status legend shows how many clusters in the view are Critical, Major, Minor, Normal, Disabled, and Unknown, with a total showing how many clusters are in the view.

Customizing the View

The **Customize** link is in the upper right corner of the cluster table view page. Click this button to determine which columns are displayed and in what order. Refer to “Customizing the Cluster Table View Page” for more information.

Cluster Collection Columns

Sort columns by clicking the column header for ascending or descending order. Place your cursor over a column name for a brief description of the column. Refer to “Customizing the Cluster Table View Page” for more information on customizing columns.

- Selection

- CS
- Cluster Name
- Cluster Address
- Cluster Type
- Cluster Description

Selection

Select the checkbox in this column to select a cluster. You can select more than one cluster. This option is available in both the table view and the tree view. Select the checkbox in the column heading to select all displayed events.

CS

The **CS** column (indicating cluster status) contains the cluster status icon for each particular cluster, a status that reflects the most severe status of all the cluster members and Cluster Monitor Resources, such as disk or CPU, for that cluster. This status is independent of the hardware and software status shown on the system table view page. For an HP Serviceguard cluster, cluster status is set to Unknown. To view the accurate state of the Serviceguard cluster status, HP Serviceguard Manager should be used. For MSCS clusters, the status is the most critical cluster status displayed in Cluster Monitor. This status is determined by the threshold (CPU, Disk) status and the node status of the cluster nodes that are retrieved by the HP Insight Management Agent (if available). For all other types of clusters, the status is determined by the most critical of the threshold (CPU, Disk) statuses and the node statuses of the cluster nodes retrieved by the Insight Management Agent (if available).

Cluster Name

The **Cluster Name** column contains the cluster name. When you place the cursor over the cluster name, the full system DNS name is shown. If you click the cluster name of an MSCS cluster, the Cluster Monitor page displays. Refer to “Cluster Monitor” for more information. If the cluster selected is an HP Serviceguard cluster, a new cluster table view page appears, showing the servers in the cluster. From this list, click a server name to access the **System Page** for that server. If the cluster is of any other type, the **System Page** for that cluster appears. Refer “Identity Tab for Clusters” for more information.

Cluster Address

The **Cluster Address** column contains the IP address for the cluster.

Note:



HP Serviceguard clusters do not have an IP address. Therefore, this column is blank for this type of cluster.

Cluster Type

The **Cluster Type** column shows the cluster type. Some of the cluster types supported include:

- MSCS
- OpenVMS

- UnixWare
- Novell NetWare
- Oracle RAC
- Tru64 UNIX
- HP Serviceguard

Cluster Description

The **Cluster Description** column contains a description of that cluster type. HP Serviceguard clusters have a description of **HP Serviceguard cluster**.

Buttons

Three buttons at the bottom of the page are available to users with full-configuration-rights:

- **Save Selection As.** When clusters are selected, you can save the selection with a new name. Changes are saved on a per-user, per-collection basis. Refer to “Saving Collections” for more information.
- **Delete.** This button is used to delete clusters from the database. Select clusters to delete from the database, and click **Delete**. A confirmation box appears. Click **OK** to delete the clusters, or click **Cancel** to cancel the deletion. Refer to “Deleting Clusters from the Database” for more information.
- **Print.** When the report is displayed, select **File->Print** from the browser menu to print the report.

Note:

Because the following print options are not supported in HP SIM, you cannot:

- Change the **Orientation** to **Landscape** in the **Print** dialog box (refer to **Printing Problems** in “Printing” for a workaround to this issue)
- Cancel printing after the print job has been executed, but you can access the operating systems print queue and cancel the print job
- Print to a file
- Print selected clusters, not entire list of clusters
- Printing the cluster table view page if you close the browser immediately after issuing a print request



Buttons are disabled if you do not have appropriate rights. However, the **Print** button appears for all users.

Related Procedures

- Customizing the Cluster Table View Page
- Deleting Clusters from the Database
- Saving Collections
- Printing a Cluster Collection Report

Related Topics

- Cluster Table View Page
- Cluster Monitor
- HP Serviceguard Manager Overview

Customizing the Cluster Table View Page

Perform the following procedure to customize the cluster table view page to determine the columns to display and the sort order.

To customize the cluster table view page:

1. On the cluster table view page, click **Customize**. The **Customize Table Appearance**.
2. Select the columns you want displayed from the **Available Columns** box, and click >> to add the columns to the **Displayed Columns** box.
3. If you want to remove one or more columns from the display, select the columns in the **Displayed Columns** box, and click << to move them to the **Available Columns** box so they are no longer be displayed.
4. To sort the list by a particular column, select a column from the **Sort by** dropdown list.
5. Select **Ascending** or **Descending**.
6. If you want the customization to apply to all cluster collections, select **Apply to all cluster collections**.
7. Click **OK** to save selections and return to the cluster table view page, or click **Cancel** to cancel all changes and return to the cluster table view page.

Related Procedures

- Saving Collections
- Deleting Clusters from the Database
- Printing a Cluster Collection Report

Related Topics

- Cluster Table View Page
- Navigating the Cluster Table View Page

Deleting Clusters from the Database

Perform the following procedure to delete one or more clusters from the HP SIM database.

Note:



Clusters that contain cluster members defined in HP Systems Insight Manager (HP SIM) cannot be deleted. To delete a cluster with its cluster members, you must first go to the system table view page by selecting the **All Systems** collection in the **Systems and Events** panel. Then, select the cluster along with all of its members and click **Delete**.

To delete clusters:

1. On the cluster table view page, select one or more clusters to delete from the database by highlighting them in the display.
2. Click **Delete**. A dialog box is displayed, stating, *Are you sure you want to delete these systems?*
3. Click **OK** to delete the clusters, or click **Cancel** to return to the cluster table view page without deleting the clusters.

Related Procedures

- Saving Collections
- Printing a Cluster Collection Report
- Customizing the Cluster Table View Page

Related Topics

- Cluster Table View Page
- Navigating the Cluster Table View Page

Printing a Cluster Collection Report

Use the following procedure to view and print a cluster collection report.

To view and print cluster collection results reports:

1. From the cluster table view page, select the clusters that you want to include in the report.
2. Click **Print** to print the report.
3. When the report is displayed, select **File>Print** from the browser menu to print the report.

Because the following print options are not supported in HP Systems Insight Manager (HP SIM), you cannot:

- Change the **Orientation** to **Landscape** in the **Print** dialog box (refer to **Printing Problems** in “Troubleshooting” for a workaround to this issue)
- Cancel printing after the print job has been executed, but you can access the operating systems print queue and cancel the print job
- Print to a file

- Print selected clusters, not entire list of clusters
- Print the cluster table view page if you close the browser immediately after issuing a print request

Related Procedures

- Customizing the Cluster Table View Page
- Deleting Clusters from the Database
- Saving Collections
- Printing a Cluster Collection Report

Related Topics

- Cluster Table View Page
- Navigating the Cluster Table View Page

Event Table View Page

To access **Events**, click **Events** in the **Systems and Events** panel. Users with full-configuration-rights can manage all shared event collections from the event table view page. Users can manage their own private event collections from this page as well. They can:

- **Clear events.** Select one or more events to clear, and click **Clear**.
- **Delete events.** Select one or more events to delete, and click **Delete**.
- **Assign events.** Select one or more events to assign to specific users, and click **Assign to**.
- **Add comments to events.** Select one or more events to add comments to, and click **Enter Comment**.
- **Print event collection results.** Click **Print** to print the collection results.
- **Customize the view.** Click **Customize** to customize which columns are displayed and in what order. Refer to “Customizing the Event Table View Page” for more information.

Related Procedures

- Clearing Events from the Collection
- Deleting Events from the Database
- Assigning Events to Users
- Entering Comments on Events
- Printing an Event Collection Report

Related Topics

- Navigating the Event Table View Page
- Monitoring Systems, Clusters, and Events
- Event Severity Types
- Event Details Section

Navigating the Event Table View Page

The event table view page is a list of events that meet common criteria. For example, if you open an event collection from the events table view page by **Event Type**, you can view systems that have generated the same events.

The event table view page is divided into the following sections:

1. Event Status Legend
2. Event Collection Columns
3. Event Details
4. Event Management Buttons
5. Customizing the View

The screenshot shows the 'All Events' page with a summary of 4469 events: 1796 Critical, 12 Major, 75 Minor, 0 Warning, 1706 Normal, and 876 Informational. The table below shows the following data:

State	Severity	Event Type	System Name	Event Time	Assigned To
Not cleared	Normal	System is reachable	zoe11	6/14/05 9:12 PM	
Cleared	Critical	System is unreachable	zoe11	6/14/05 9:07 PM	
Not cleared	Informational	Successful Login	nirbudemo	6/14/05 9:02 PM	
Not cleared	Critical	System is unreachable	gatoC	6/14/05 9:02 PM	
Not cleared	Normal	System is reachable	zoe11	6/14/05 8:53 PM	
Cleared	Critical	System is unreachable	zoe11	6/14/05 8:46 PM	
Not cleared	Critical	System is unreachable	851	6/14/05 8:13 PM	
Not cleared	Normal	System is reachable	851	6/14/05 8:02 PM	
Cleared	Critical	System is unreachable	851	6/14/05 7:56 PM	
Not cleared	Normal	System is reachable	zoe11	6/14/05 7:56 PM	
Cleared	Critical	System is unreachable	zoe11	6/14/05 7:53 PM	
Not cleared	Critical	System is unreachable	leejohns	6/14/05 7:51 PM	
Not cleared	Critical	System is unreachable	muxp7	6/14/05 7:51 PM	
Not cleared	Normal	System is reachable	hasup23	6/14/05 7:32 PM	

From this page, you can clear, delete, and assign events, enter comments on the event, and view printable reports.

Event Status Legend

The legend shows how many events in the view are Critical, Major, Minor, Normal, and Informational. Refer to “Event Severity Types” for more information on event status types.

Event Details

The event collection can be displayed by clicking:

- An event collection from the **Systems and Events** panel
- An event status icon in the **System Status** panel
- The **All Events Associated with this System** link from the **System Page**
- A private event collection

- A hyperlink in the **Uncleared Events** section on the **System Overview** page

Event collections are filtered based on authorizations. Users can only view events on systems for which they have the appropriate authorization. Refer to “Users and Authorizations” for more information.

When HP Storage Essentials is installed, a link in this section allows you to view the corresponding event details in HP Storage Essentials.

Event Collection Columns

Sort collection results by a particular column, click the column header for ascending or descending order. Place your cursor over a column name for a brief description of the column. Refer to:

- Selection
- State
- Severity
- Event Type
- System Name
- Event Time
- Assigned To
- Comments

Selection

Select the checkbox in this column to select an event. You can select more than one event. Select the checkbox in the column heading to select or deselect all displayed events.

State

This column displays whether the event is in the Cleared or Not Cleared state. Events start in the Not Cleared state. A Cleared state means the user is no longer interested in this event. Event states also include In Progress, indicating not all the data for the event has been logged. Events in an In Progress state cannot be removed or cleared. A restart of the CMS moves any pending state events to Not Cleared.

Severity

This column displays the event status icon to indicate the severity of a problem represented by the event. Refer to “Event Severity Types” for more information.

Event Type

This column displays the type of an event. Some examples are SNMP traps, login failures, or the replicate agent settings tool event type. Select an event type from the list to view the **Event Details** section. The information displayed varies depending on the event. If you cannot see the entire event type in the column, place your cursor over a this field, and a popup window is displayed that shows the entire event type. Refer to “Event Details Section” for more information on event details.

System Name

This column displays the system name on which the event occurred. Clicking a link in this column displays the **System Page** for the selected system.

When an event occurs that affects an entire rack or enclosure, it is possible for several systems in that rack or enclosure to generate a trap for that event. These container traps are filtered such that only one event is logged per rack or enclosure trap. Also, even though the source of the trap is a server blade or management processor, HP Systems Insight Manager (HP SIM) sets the **Event Source** and **Associated System** for the logged event to the rack or enclosure, as appropriate. Refer to “About Racks and Enclosures” for more information on racks and enclosures.

Event Time

This column displays the time stamp when the CMS received this event, which includes the date and time. If the client is in a different time zone than the event time (CMS time), the event time is converted to the client time zone.

Assigned To

To assign responsibility for an event to a user, select the event, and click **Assign to** at the bottom of the page. The **Assign to** section appears, which enables you to select to assign a new assignee or use an existing assignee. If you select to use an existing assignee, you can only select one user name from the list. This name does not have to be a user with privileges on the system or a name that can be used to log into the CMS. This field is free-form text. Refer to “Assigning Events to Users” for more information on assigning an event to a user.

Comments

This column displays the comments for this event or is blank if no comments have been entered. Comments are truncated in the column itself. Click the event type to view the entire comment if needed, or place your cursor over a comment field, causing a pop-up window that shows the entire comment to appear. Refer to “Entering Comments on Events” for adding comments.

Event Management Buttons

Five buttons at the bottom of the event table view page are available to users with full-configuration-rights only. These buttons might not appear depending on where you access this page from. For example, when creating a task and selecting targets, there are no buttons displayed, only the table or system names.

- **Clear.** This button is used to clear one or more events from the database. Select the events to clear, and click **Clear**. Refer to “Clearing Events from the Collection” for more information.
- **Delete.** This button is used to delete one or more events from the database. Select the events to be deleted, and then click **Delete**. A dialog box appears. Click **OK** to continue with the deletion, or click **Cancel** to cancel the deletion. Refer to “Deleting Events from the Database” for more information.
- **Assign to.** This button is used to assign responsibility for events to a particular user. Refer to “Assigning Events to Users” for more information.
- **Enter Comments.** Brings up a dialog box to enter comments for one or more events. Refer to “Entering Comments on Events” for more information.
- **Print.** When the report is displayed, select **File->Print** from the browser menu to print the report.

Note:

Because the following print options are not supported in HP SIM, you cannot:



- Change the **Orientation** to **Landscape** in the **Print** dialog box (refer to **Printing Problems** in “Printing” for a workaround to this issue)
- Cancel printing after the print job has been executed, but you can access the operating systems print queue and cancel the print job
- Print to a file
- Print selected events, not entire list of events
- Print the event table view page if you close the browser immediately after issuing a print request

Buttons are disabled if you do not have appropriate privileges. However, the print button is displayed for all users.

Customizing the View

The **Customize** link is in the upper right corner of the event table view page. Click this link to determine which columns are displayed and in what order. The **Customize** link is not shown on the following pages:

- **System Overview**
- **Advanced Search**
- **System Page** under the **Events** tab
- The **Task** page, when selecting targets

Refer to “Customizing the Event Table View Page” for more information.

Related Procedures

- Customizing the Event Table View Page
- Clearing Events from the Collection
- Deleting Events from the Database
- Assigning Events to Users
- Entering Comments on Events
- Printing an Event Collection Report

Related Topics

- Monitoring Systems, Clusters, and Events
- Event Severity Types

Customizing the Event Table View Page

Perform the following procedure to customize the event table view page to determine the columns to display and the sort order.

To customize the event table view page:

1. On the event table view page, click **Customize**. The **Customize Table Appearance** page is displayed.
2. Select the columns you want displayed from the **Available Columns** box, and click >> to add the columns to the **Displayed Columns** box.
3. To rearrange how the columns display, select a column in the **Displayed Columns** box, and click **Move Up** or **Move Down**.
4. To remove columns from the display, select the columns in the **Displayed Columns** box, and click << to move them to the **Available Columns** box so they will no longer be displayed.
5. To sort the collection by a particular column, select a column from the **Sort by** dropdown list.
6. Select **Ascending** or **Descending**.
7. To apply the customization to all event collections, check **Apply to all event collections**.
8. Click **OK** to save selections and return to the event table view page, or click **Cancel** to cancel all changes and return to the event table view page.

Related Procedures

- Clearing Events from the Collection
- Deleting Events from the Database
- Assigning Events to Users
- Entering Comments on Events
- Printing an Event Collection Report

Related Topics

- Event Table View Page
- Navigating the Event Table View Page

Clearing Events from the Collection

Perform the following procedure to clear events. Only users with full-configuration-rights can clear events.

To clear an event:

1. On the event table view page, select the event that you want to clear.
2. Click **Clear**. For the events selected, the state changes from Not Cleared to Cleared in the **State** column.

Related Procedures

- Customizing the Event Table View Page
- Deleting Events from the Database
- Assigning Events to Users
- Entering Comments on Events
- Printing an Event Collection Report

Related Topics

- Navigating the Event Table View Page
- Event Table View Page
- Event Details Section

Deleting Events from the Database

Perform the following procedure to delete events. You must have full-configuration-rights to delete events.

Pending events, discovered system events, and service events cannot be deleted.

To delete an event:

1. On the event table view page, select the event you want to delete.
2. Click **Delete**. A confirmation box is displayed.
3. Click **OK** to delete the event, or click **Cancel** to return to the event table view page.

Related Procedures

- Customizing the Event Table View Page
- Clearing Events from the Collection
- Assigning Events to Users
- Entering Comments on Events
- Printing an Event Collection Report

Related Topics

- Navigating the Event Table View Page
- Event Table View Page
- Event Details Section

Assigning Events to Users

Use the following procedure to assign a single event or multiple events to one or more users. Only users with full-configuration-rights can assign events from shared collections.

Caution:



If events that are selected have previously been assigned, selecting a new assignee and clicking **OK** overrides the previous assignment.

Note:



A maximum of 50 characters can be entered for **Assignee**.

To assign an event to a user:

1. On the event table view page, select the events that you want to assign to a user.
2. Click **Assign To**. The **Assign to** section displays.
3. Select **New assignee** or **Choose existing assignee**. If you select **Choose existing assignee**, click the down arrow, and select an assignee from the dropdown list.
4. Click **OK** to update the database, or click **Cancel**.

Related Procedures

- Clearing Events from the Collection
- Deleting Events from the Database
- Entering Comments on Events
- Printing an Event Collection Report
- Customizing the Event Table View Page

Related Topics

- Navigating the Event Table View Page
- Event Table View Page

Entering Comments on Events

Use the following procedure to add comments to events. Only users with full-configuration-rights can add comments to events.

Caution:



If you select multiple events in which to add comments, any previous comments are replaced in the database.

Note:



The maximum number of characters allowed for comments is 1,000.

To add comments to an event:

1. On the event table view page, select the events for which you want to enter comments.
 2. Click **Enter Comments**. The **Enter Comments** section displays.
 3. Enter the comments and click **OK** to update the database, or click **Cancel** to return to the event table view page.
-

Note:



Comments that are added to events in HP Systems Insight Manager (HP SIM) are not transferred to HP Storage Essentials.

Related Procedures

- Customizing the Event Table View Page
- Clearing Events from the Collection
- Deleting Events from the Database
- Assigning Events to Users
- Printing an Event Collection Report

Related Topics

- Navigating the Event Table View Page
- Event Table View Page
- Event Details Section

Printing an Event Collection Report

Perform the following procedure to view and print event collection reports.

To view and print event collection results reports:

1. On the event view page, click **Print**.
A printable window appears.
2. Click **Print** to print the report.
3. When the report is displayed, select **File->Print** from the browser menu to print the report.

Because the following print options are not supported in HP Systems Insight Manager (HP SIM), you cannot:

- Change the **Orientation** to **Landscape** in the **Print** dialog box, refer to “Printing” for a workaround to this issue
- Cancel printing after the print job has been executed, but you can access the operating systems print queue and cancel the print job
- Cancel printing to a file
- Print selected events, not entire list of events
- Print the event table view page if you close the browser immediately after issuing a print request

Related Procedures

- Customizing the Event Table View Page
- Clearing Events from the Collection
- Deleting Events from the Database
- Assigning Events to Users
- Entering Comments on Events

Related Topics

- Navigating the Event Table View Page
- Event Table View Page
- Event Details Section

Event Severity Types

HP Systems Insight Manager (HP SIM) reports the following severity levels for events:

Status Icon	Icon Meaning	Description
	Critical	Events of this type indicate a failure and signal the need for immediate attention.
	Major	Events of this type indicate an impending failure.
	Minor	Events of this type indicate a warning condition that can escalate into a more serious problem.
	Normal	Events of this type indicate that this event is not a problem.
	Unknown	Events of this type indicate that this event is an unknown severity or unknown problem.

Status Icon	Icon Meaning	Description
	Warning	Currently in a state that might become a problem. Note: In HP SIM 5.0, only WBEM indications map to warning.
	Informational	Events of this type require no attention and are provided as useful information.

Related Topics

- [Event Table View Page](#)
- [Navigating the Event Table View Page](#)

Event Details Section

Introduction

When you click a link in the **Event Type** column on the event table view page, the **Event Details** section is displayed, providing detailed information about the particular event. Events are generated from SNMP traps, HyperText Transfer Protocol (HTTP) events, or internally generated events.

Note:



Events can be generated from Web-Based Enterprise Management (WBEM) if you have subscribed to WBEM events on the managed system. Refer to “Subscribing to WBEM Indications” for more information on subscribing to WBEM events.

Note:



Events are tracked only for systems that have been discovered. Refer to Automatic Discovery, refer to the “Configuring Automatic Discovery” for more information on configuring and running Automatic Discovery.

Event Details

This section identifies the following information about the event:

- **Event Severity.** Displays the severity of the event
- **Cleared Status.** Shows if the event is Cleared, Not Cleared, or Unknown
- **Event Source.** Displays the system on which the event originated
- **Associated System.** Displays the system that generated the event

- **Associated System Status.** Shows the current status of the system that generated the event that changes as the status of the system changes
- **Event Time.** Displays the time the event was received by the central management server (CMS)
- **Description.** Explains the source or type of event, which can be an SNMP trap, a DMI indication, or an internally generated message, such as the discovery of a system
- **Assignee.** Displays the user to which the event has been assigned
- **Comments.** Displays comments entered by a user

Depending on the event type, the following information displays in the **Details** box:

- Servers in Enclosure
For enclosure events, this section lists all of the servers in the affected enclosure.
- Enclosures in Rack
For rack events, this section lists all of the enclosures in the affected rack.
- Trap Details
 - Date and time the event occurred
 - Event Description
 - Trap Information
- Discovered System Details
- Discovered Date
- Event Details
 - User name
 - System name of the remote system from where the user was browsing
 - IP address of the system from where the user was browsing

Note:



System name and IP address are not provided for the Unauthorized User Account Modified Event. It is an event internally generated by the HP Systems Insight Manager (HP SIM) Server.

- Change Details
 - Source of current status change
 - Previous severity

- Task Details
 - Time the task ran
 - User that ran the task
 - Systems on which the task ran

- Status Change Details
 - **Subsystem Name.** For example, memory, processor, and storage
 - **Previous Subsystem status.** The status of the subsystem before the event
 - **Overall Performance status.** The combined status of all the subsystems (the worst subsystem status)
 - **Explanation.**

Click **View Printable Details** to view the details in printable format. Click **File->Print** to print the details.

Related Topics

- Navigating the Event Table View Page
- Event Table View Page

Searching for Systems and Events

Two types of searches can be performed in HP Systems Insight Manager (HP SIM). There is a basic search, which searches on a system name, and an advanced search.

To perform a basic search:

1. In the **Search** panel, enter a system name or key word.
2. Click **Search**. The **Search Results** page appears.

To perform an advanced search:

1. In the **Search** panel, click **Advanced Search**.
2. Select **systems**, **events**, or **clusters** and select any defining criteria.
3. Click **View**. The **Search Results** page appears.

Related Procedures

- Performing a Basic Search
- Saving Collections
- Performing an Advanced Search for Systems
- Performing an Advanced Search for Clusters
- Performing an Advanced Search for Events

Related Topics

- Basic and Advanced Search
- Search Criteria

Basic and Advanced Search

Basic Search

The Search feature enables you to quickly retrieve details about a system using its name or common system attributes. The search field only allows the following characters to be entered: letters, numbers, tilde, dash, period, underscore, apostrophe, and space. Click **View** to search for the indicated system.

The **Search Results** displays a list of systems in the database whose names closely resemble the target name. This list of system names is hyperlinked. Clicking a name in the list displays the **System Page** for that system.

If no systems in the database resemble the target system, the **Search Results** indicate that no entries meet the criteria and gives you the option to search again by performing an advanced search.

Advanced Search

To access the **Advanced Search** page, click the **Advanced Search** hyperlink in the **Search** panel.

You can create a system, event, or cluster search by selecting various options in the search type selection box at the top of the **Advanced Search** page. Then you can specify the criteria to be used in the search. If you make selections in a particular box, the values offered in the subsequent selection boxes are updated as appropriate. The result of running a search is a collection. The criteria selected can also be saved as a collection, so the search can be run again at a later date. The saved collections are stored in the **Systems and Events** panel as **Systems** or **Events**. These collections can be saved as private or shared.

Hierarchical Displays

Some search criteria require hierarchical displays. Examples of hierarchical criteria are Operating System, Event Type, and Software/Firmware.

In these cases, the comparison selection box is replaced by a selection box containing the appropriate English for that particular tree level. The most complex of these cases is the Software/Firmware criteria. When Software/Firmware is selected, a series of search criteria are added below in a tree format:

- system type is
- and operating system is
- and software/firmware type is
- and name is
- and version is

In this case, as selections are made in the higher-level selection boxes, the available selections in lower-level boxes update.

Save As

When you click **Save As**, the **Save Collection As** section displays. Enter a name for the search in the **Name** field, and select where to save it. Refer to “Saving Collections” for more information.

View

When you click **View**, the results of the search displays below the search frame. This functionality enables you to preview the results of the search before saving it or to run a search without saving it.

Related Procedures

- Performing a Basic Search
- Saving Collections
- Performing an Advanced Search for Systems
- Performing an Advanced Search for Clusters
- Performing an Advanced Search for Events

Related Topic

- Searching for Systems and Events

Performing a Basic Search

Perform this procedure to complete a basic system search by searching for matches in system name and common system attributes.

To perform a basic search:

1. In the **Search** panel, enter a system name.
2. Click **Search**. The **Search Results** page appears where you can search for matches in system name and common system attributes.
3. From the **Search Results** page, use the same system name, or change the system name in the **Search again** field.
4. If you change the system name, click the down arrow in the **in** box, and select **system name** or **common system attribute**.

Note: Common system attributes include Full DNS name, Device hostname, Serial number, Operating System Type, Operating System Version, Operating System description, Operating System name, Product model, System type, and IP address.

5. Click **View**. The new **Search Results** are displayed.
6. After the search results display, you can:
 - Save the search results. Click **Save As**, enter a name for the search, and select where to save the collection. Refer to “Saving Collections” for more information. Click **OK** to save the search, or click **Cancel** to return to the **Search Results** page.

- Perform a more advanced search. Click **Advanced**. The **Advanced Search** page displays. Refer to “Basic and Advanced Search” for more information on the Advanced Search option.

Related Procedures

- Saving Collections
- Performing an Advanced Search for Systems
- Performing an Advanced Search for Events
- Performing an Advanced Search for Clusters

Related Topics

- Searching for Systems and Events
- Basic and Advanced Search
- Search Criteria

Performing an Advanced Search for Systems

Perform the following procedure to complete an advanced search for systems. The following images shows the **Advanced Search** page for systems.

The screenshot shows the 'Advanced Search' window with the following configuration:

- Search for:** systems
- Criteria 1:** where system name is (any)
- Criteria 2:** and system type is Server
- Criteria 3:** and operating system name is Microsoft Windows Server 2003, Sp5 and version is 5.2

Buttons visible include 'Delete' for each criterion, 'Add', 'View', and 'Save As'.

To search for systems:

1. Click **Advanced Search** in the **Search** panel.
2. Select **systems** from the **Search for** dropdown list.
3. From the first selection box (criteria selection), click the down arrow, and select the search criteria.
4. From the second selection box (comparison selection), click the down arrow, and select the comparison option.

Note: Different criteria support different comparisons. The comparison options change with the criteria selected. For example, if you select **operating system** as a criterion, the possible comparisons available are: is, is not, contains, starts with, and ends with. Refer to “Search Criteria” for more information.

5. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select the value from the dropdown list, or enter the needed information in the input box supplied.

6. Click **Add** to add additional criteria, click **View** to conduct the system search immediately, or click **Save As** to save the search as a collection. Refer to “Basic and Advanced Search” for more information on **Go** and **Save as**.

Note: Criteria are re-ordered after clicking **View** or **Save As**. If criteria types are the same they are OR'd together and if they are different, they are AND'd together.

7. If you clicked **View**, the results are displayed. You can make selections to delete or print the results. Refer to “Deleting System Search Results” for more information on deleting selections. Refer to “Printing System Search Results” for information on printing search results.

Related Procedures

- Deleting System Search Results
- Printing System Search Results
- Saving Collections
- Performing an Advanced Search for Events
- Performing an Advanced Search for Clusters
- Performing a Basic Search

Related Topics

- Searching for Systems and Events
- Basic and Advanced Search
- Search Criteria

Deleting System Search Results

Perform the following procedure to delete one or more systems from a system search before saving.

Note:



Deleting many systems from the list results in a performance delay.

To delete systems from a search view:

1. After performing a search, the search results are displayed.
2. Select systems to delete from the search, and click **Delete**. A dialog box appears stating *Are you sure you want to delete these systems?*
3. Click **OK** to delete the systems, or click **Cancel** to return to the **Search Results** page without deleting the systems.

Related Procedures

- Performing an Advanced Search for Systems
- Printing System Search Results

Related Topic

- Searching for Systems and Events

Printing System Search Results

Perform the following procedure to print the system search results.

To print system search results:

1. After performing a search, the **Search Results** page appears.
2. Click **View**. The results are displayed.
3. Click **Print**.

The results are printed.

Note: The **Print** dialog box could be hidden. If so, go to the Windows Task Bar to display the box.

Because the following print options are not supported in HP Systems Insight Manager (HP SIM), you cannot:

- Change the **Orientation** to **Landscape** in the **Print** dialog box, refer to “Printing” for a workaround to this issue
- Cancel printing after the print job has been executed, but you can access the operating systems print queue and cancel the print job
- Cancel printing to a file
- Print selected systems, only the entire list of systems
- Print the system search results if you close the browser immediately after issuing a print request

Related Procedures

- Saving Collections
- Deleting System Search Results

Related Topic

- Performing an Advanced Search for Systems

Performing an Advanced Search for Events

Perform the following procedure to search for events. The following images shows the **Advanced Search** page for events.

Note:



You can quickly display all service events with the **Any** type by selecting **Systems->Events->Shared->Service Events->All HP Service Events** from the **Systems and Events** panel.

To search for events:

1. Click **Advanced Search** in the **Search** panel.
2. Select **events** from the **Search for** dropdown list.
3. From the first selection box (criteria selection), click the down arrow, and select the search criteria.

Note: If you selected **event type**, refer to “Event Type Criterion” for more information.

4. From the second selection box (comparison selection), click the down arrow, and select the comparison option.

Note: Different criteria support different comparisons. The comparison options change with the criteria selected. For example, if you select **operating system** as a criterion, the possible comparisons available are: is, is not, contains, starts with, and ends with.

5. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select the value from the dropdown list, or enter the needed information in the input box supplied.
6. Click **Add** to add additional criteria, click **View** to conduct the event search immediately, or click **Save as** to save the search as a list. Refer to “Basic and Advanced Search” for more information on **Go** and **Save as**.
7. If you clicked **View**, the results are displayed. You can make selections to delete or print the results. Refer to “Deleting System Search Results” for more information on deleting selections. Refer to “Printing System Search Results” for information on printing search results.

Note: To search for new event types generated by HTTP events, select events by Event Category, and then select the event type from the **and type is** list.

Related Procedures

- Saving Collections
- Deleting Event Search Results
- Printing Event Search Results

Related Topic

- Searching for Systems and Events
- Basic and Advanced Search
- Search Criteria

Deleting Event Search Results

Perform the following procedure to delete one or more events from an event search before saving.

Note:



Deleting many events from the list results in a performance delay.

To delete events from a search view:

1. After performing a search, the search results are displayed.
2. Select events to delete from the search, and click **Delete**. A dialog box appears stating *Are you sure you want to delete these systems?*
3. Click **OK** to delete the events, or click **Cancel** to return to the **Search Results** page without deleting the events.

Related Procedures

- Performing an Advanced Search for Events
- Printing Event Search Results

Related Topic

- Searching for Systems and Events

Printing Event Search Results

Perform the following procedure to print the event search results.

To print event search results:

1. After performing a search, the **Search Results** page appears.
2. Click **View**. The results are displayed.

3. Click **Print**.

The results are printed.

Note: The **Print** dialog box could be hidden. If so, go to the Windows Task Bar to display the box.

Because the following print options are not supported in HP Systems Insight Manager (HP SIM), you cannot:

- Change the **Orientation** to **Landscape** in the **Print** dialog box, refer to “Printing” for a workaround to this issue
- Cancel printing after the print job has been executed, but you can access the operating systems print queue and cancel the print job
- Cancel printing to a file
- Print selected events, only the entire search results
- Print the event search results if you close the browser immediately after issuing a print request

Related Procedures

- Saving Collections
- Deleting Event Search Results

Related Topic

- Performing an Advanced Search for Events

Performing an Advanced Search for Clusters

Use the following procedure to search on clusters. The following images shows the **Advanced Search** page for clusters.

To search for clusters:

1. Click **Advanced Search** in the **Search** panel.
2. Select **clusters** from the **Search for** dropdown list.
3. From the first selection box (criteria selection), click the down arrow, and select the search criteria.

4. From the second selection box (comparison selection), click the down arrow, and select the comparison option.

Note: Different criteria support different comparisons. The comparison options change with the criteria selected.

5. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select the value from the dropdown list, or enter the needed information in the input box supplied.
6. Click **Add** to add additional criteria, click **View** to conduct the cluster search immediately, or click **Save As** to save the search as a collection. Refer to “Basic and Advanced Search” for more information on **Go** and **Save as**.
7. If you clicked **View**, the results are displayed. You can make selections to delete or print the results. Refer to “Deleting System Search Results” for more information on deleting selections. Refer to “Printing System Search Results” for information on printing search results.

Related Procedures

- Saving Collections
- Deleting Cluster Search Results
- Printing Cluster Search Results

Related Topics

- Searching for Systems and Events
- Basic and Advanced Search
- Search Criteria

Deleting Cluster Search Results

Perform the following procedure to delete one or more clusters from a cluster search before saving.

Note:



Deleting many clusters from the collection results in a performance delay.

Note:



Clusters that contain cluster members cannot be deleted. To delete a cluster with its cluster members, you must first go to the system table view page by selecting the **All Systems** collection in the **Systems and Events** panel. Then, select the cluster along with all of its members and click **Delete**.

To delete clusters from a search view:

1. After performing a search, the search results are displayed.
2. Select clusters to delete from the search, and click **Delete**. A dialog box appears stating *Are you sure you want to delete these systems?*
3. Click **OK** to delete the systems, or click **Cancel** to return to the **Search Results** page without deleting the clusters.

Related Procedures

- Performing an Advanced Search for Clusters
- Printing Cluster Search Results

Related Topic

- Searching for Systems and Events

Printing Cluster Search Results

Perform the following procedure to print the cluster search results.

To print cluster search results:

1. After performing a search, the **Search Results** page appears.
2. Click **View**. The results are displayed.
3. Click **Print**.

The results are printed.

Note: The **Print** dialog box could be hidden. If so, go to the Windows Task Bar to display the box.

Because the following print options are not supported in HP Systems Insight Manager (HP SIM), you cannot:

- Change the **Orientation** to **Landscape** in the **Print** dialog box, refer to “Printing” for a workaround to this issue
- Cancel printing after the print job has been executed, but you can access the operating systems print queue and cancel the print job
- Cancel printing to a file
- Print selected clusters, only the entire search results
- Print the cluster search results if you close the browser immediately after issuing a print request

Related Procedures

- Saving Collections
- Deleting Cluster Search Results

Related Topic

- Performing an Advanced Search for Clusters

Search Criteria

You can select from many criteria when you create a collection. Although the task you run is associated with one collection, one collection can include numerous conditions.

You can also exclude criteria. For example, including all systems of the type server and excluding all systems of a certain processor type provides a more distinct subset of the servers on the network. This filtering is done by selecting **is** or **is not** comparison selections.

The more commonly used criteria include system type, IP address, product name, and hardware status. Less frequently used criteria include event category (trap categories), processor, management protocol, and memory range. Event collections include both system criteria and event criteria. Event criteria do not apply to system collections.

When you select multiple criteria, the system must meet all criteria for the system to be included in the collection. For example, if you select systems within a specified IP range and with more than 32 MB of RAM, the collection does not return a system in the specified IP range if the system has less than 32 MB of RAM.

Complex collections with many individual system selections or with many different selection criteria take more system resources to execute. If a task is associated with a collection, keep the collection as simple as possible to minimize the performance impacts.

System List Criteria	Finds
asset number	User defined field listing the asset number of the system
cluster membership	Systems that belong to a certain cluster
common attributes	Systems with common attributes, including: full DNS name, system hostname, serial number, operating system type, operating system version, operating system description, operating system name, product model, system type, and IP address
contact	User-defined field listing the contact for system status information
enclosure	Systems in an enclosure by a given set of enclosure names (does not include the enclosure itself)
hardware status	Systems of specified hardware status type (Critical, Disabled, Major, Minor, Normal, and Unknown)
IP address	Systems with an IP address that falls in the specified range
location	User-defined field indicating the physical location of the system

management protocol	Systems running one or more of the following protocols: HTTP, WBEM, DMI, or SNMP
memory range	Systems with memory in the specified range (refer to "Memory Range Criterion" for details)
network protocol	Systems running on IP, IPX, or both
operating system	Systems with specific operating system, version number, or both
processor	Systems with the specified processor type, speed, or both
product name	Systems with the specified product names.
rack	Systems in a rack by a given set of rack names (does not include the rack itself)
serial number	User-defined field that displays the serial number of the system
server role	Systems that have a certain server role set on them (refer to "Server Role Criterion" for more information)
software/firmware	Systems with specific software or firmware version installed (refer to "Software/Firmware Criterion" for more information)
system name	Systems with a given set of system names
system subtype	Enables you to search on the product subtype field in the HP Systems Insight Manager (HP SIM) database (for example, Power Enclosure, Server Enclosure, and VM Host)
system type	Systems identified with the standard system types, including: cluster, desktop, enclosure, management processor, portable, printer, remote access device, repeater, router, server, switch, unknown, workstation, and so on
trust status	Systems that have Web-enabled agents that trust the management console or not
web agent	Systems with specific Web-servers or Web Agents installed
Note: The preceding System Collection Criteria are also available as Event Collection Criteria on the Advanced Search page.	
Event Collection Criteria	Finds
assignee	Events that have a particular assignee assigned to them (refer to "Assignee Criterion" for more information)
cleared state	Events with a state of Cleared, Not Cleared, or In Progress but is not displayed when the page is opened in the Automatic Event Handling UI (refer to "Cleared State Criterion" for more information)
event category	Events that belong to a certain event category

event time	Events that occurred at specified times or the age of events that are greater or less than a certain number of days but is not displayed when the page is opened in the Automatic Event Handling UI
event type	Events by type grouped by categories (above), and the display is a tree of the categories with event types for each category (refer to "Event Type Criterion" for more information)
severity	Events with specified severity levels (Critical, Informational, Major, Minor, Normal, or Warning)
Cluster Collection Criteria	Finds
cluster monitor resource	Clusters with specified cluster monitor resource
cluster name	Systems that are included in a certain cluster name
cluster type	Clusters identified with the standard cluster types, including: MSCS clusters, TruCluster Production Server clusters, TruCluster Server clusters, OpenVMS clusters, Oracle RAC clusters, SCO UnixWare7 NonStop clusters, and HP Serviceguard clusters
IP address	Cluster with a specified IP address
status type	Cluster with specific cluster status levels (Critical, Major, Minor, Normal, and Unknown)

Software/Firmware Criterion

- Be sure you have access to a repository. Refer to "Version Control" for more information.
- When comparing against a ProLiant Support Pack, the only comparison you can use with a ProLiant Support Pack is **Equal To**. In addition, HP SIM cannot determine whether a ProLiant Support Pack was actually installed on a system, only whether all of the components in a ProLiant Support Pack are installed on a system. A system is returned by this search only if every component in the ProLiant Support Pack is on the list. It is unlikely that all of the components in a ProLiant Support Pack are installed on any system, so use this carefully.
- This criterion retrieves information from the SQL database table that was populated by a Software Version Status Polling Task. This table is also updated when software is installed through the Update Software or Firmware HP SIM Task. Therefore, if software was installed or uninstalled on systems without using HP SIM and after a Software Version Status Polling Task last ran, this search might not return the correct results.

Cleared State Criterion

You can run a search on a certain set of event statuses:

- **Any**. Includes all events whether they are Cleared, Not Cleared, or In Progress
- **Cleared**. Includes events that are cleared

- **Not Cleared.** Includes events that are not cleared
- **In Progress.** Includes events from tasks which are in the progress, and when the event completes, these events become Uncleared

Server Role Criterion

The Server Role criterion is a system or event collection search that enables you to list the servers of one or more matching roles. The server role is a user-specified value available on HP Insight Management Agent 5.4 or later. To create the criteria, select server role in the **Where** dropdown list on the **Advanced Search**, page and select the criteria comparison option.

Assignee Criterion

You can run a search on certain events that are assigned to a particular user. When you select the **assignee** collection criteria, the result is a scrollable list of users of which more than one can be selected.

Note:



If you do not select a user, an error message displays, stating that there are no assignees for these events. Add assignees from the event table view page.

Event Category Criterion

Event Type Criterion

Note:



Only one event type criteria can be used in a given search.

When using the event type criterion, you must select a comparison criterion such as **is** or **is not**. A tree view of the event types, organized by event category, is then displayed. Next, in the **type(s)** box, which contains the tree, select a types to search against. You can select an entire category, or click **+** to expand the branch and select individual categories, or click **-** to collapse close the branch. Click **Add** to add additional criteria, click **View** to perform the search immediately, or click **Save As** to save the search. Refer to "Saving Collections" for more information on using **Save As**.

Note:



While it is possible to select a specific version of a trap (for example, Array Accelerator Bad Data (Version. 1)), it is better to select both versions because you might have older or newer agents on some managed systems. Selecting all versions ensures that all agent versions are included in the event collection.

Memory Range Criterion

You can set the memory ranges for systems that you include in the collection. You can select multiple groups, one at a time, from the following ranges:

- **Memory Equal To (=)**. Includes systems with memory equal to a specified amount
- **Memory Not Equal To (!=)**. Includes systems with memory not equal to a specified amount
- **Memory Less Than (<)**. Includes systems with less memory than the specified amount
- **Memory Less Than or Equal To (<=)**. Includes systems with memory less than or equal to a specified amount
- **Memory Greater Than (>)**. Includes systems with more memory than the specified amount
- **Memory Greater Than or Equal To (>=)**. Includes systems with memory greater than or equal to a specified amount
- **Memory Range Between (is between)**. Includes systems with memory in the specified range

Related Topic

- Searching for Systems and Events

Reference

The Reference section for **Systems** and **Events** includes information on list naming conventions: all system-, event-, and cluster-shared collections and hidden collection names.

Related Topics

- Collection Naming Conventions
- Default Public Collections

Default Public Collections

Shared System Collections

All users can view shared collections, but only users with full-configuration-rights can create, edit, or delete shared collections.

The following shared default system collections are based on System Type:

- **All Systems.** Includes all discovered systems in the database.
- **All Servers.** Includes all discovered servers in the database.
- **All VSE Resource.** Includes all discovered Virtual Server Environment (VSE) resources in the database.

The following are included under **All VSE Resources**:

- **All nPartition Servers.** Includes all discovered systems by type with a Complex type
 - **All HP Integrity Virtual Machines.** Includes all discovered systems by type with a Server type and HP Integrity Virtual Machine Host subtype
 - **All Virtual Partition Servers.** Includes all discovered systems by type with a Server type and HP Virtual Partition Server subtype
 - **All Resource Partitions.** Includes all discovered systems by type with a Resource Partition type
 - **All Shared Resource Domains.** Includes all discovered systems by type with a Shared Resource Domain type
 - **All HP Serviceguard Clusters.** Includes all discovered systems by type with a Cluster type and an HP Serviceguard subtype
 - **All Standalone Servers.** Includes all discovered systems by type that are HP/9000 or Integrity standalone systems
- **HP BladeSystem.** Includes all discovered blades in the database

The following are included under **HP BladeSystem**:

- **All p-Class Racks.** Includes all racks with HP BladeSystem-Class subtypes
 - **All e-Class Enclosures.** Includes all enclosures with HP BladeSystem e-Class/CCI subtypes
 - **Spare Systems.** If HP ProLiant Essentials Automation Manager is installed, this collection includes Spare Blade Servers that could be utilized for recovery of failed Blade Servers. For more information, refer to “HP ProLiant Essentials Automation Manager Overview”.
 - **Systems Needing Maintenance.** If HP ProLiant Essentials Automation Manager is installed, this collection includes any failed Blade Server that was previously under HP ProLiant Essentials Automation Manager's control and now requires maintenance. For more information, refer to “HP ProLiant Essentials Automation Manager Overview”.
- **Storage Systems.** Includes all discovered storage systems in the database

The following are included under **Storage Systems**:

- **All Storage Systems.** Includes all discovered storage systems in the database.
- **All Storage Hosts.** Includes all discovered storage hosts in the database.

- **All Storage Switches.** Includes all discovered storage switches in the database.
- **All Storage Arrays.** Includes all discovered storage arrays in the database.
- **All Tape Libraries.** Includes all discovered tape libraries in the database.

- **All Racks.** Includes all discovered racks in the database.
- **All Enclosures.** Includes all discovered enclosures in the database
- **All Clients.** Includes all discovered clients in the database
- **All Networking Devices.** Includes all discovered networking systems in the database, which, include routers, switches, repeaters, and remote access systems
- **All Printers.** Includes all discovered printers in the database
- **All Management Processors.** Includes all discovered management processors in the database

The following collections are based on System by Status:

- **Critical Systems.** Includes all systems in the database with Critical status
- **Major Systems.** Includes all systems in the database with Major status
- **Minor Systems.** Includes all systems in the database with Minor status
- **Normal Systems.** Includes all systems in the database with a Normal status
- **Disabled Systems.** Includes all systems in the database with a Disabled status

The following collections are based on Systems by Operating System:

- **HP-UX.** Includes all systems in the database that have an operating system equal to HP-UX
- **Microsoft Windows Server 2003.** Includes all systems in the database that have an operating system equal to Microsoft Windows Server 2004
- **Microsoft Windows 2000.** Includes all systems in the database that have an operating system equal to Microsoft Windows 2000
- **Microsoft Windows NT.** Includes all systems in the database that have an operating system equal to Microsoft Windows NT
- **Novell Netware.** Includes all systems in the database that have an operating system equal to Novell Netware
- **SCO UNIX.** Includes all systems in the database that have an operating system equal to SCO UNIX
- **Microsoft Windows XP.** Includes all systems in the database that have an operating system equal to Microsoft Windows XP
- **Microsoft Windows 95, 98, ME.** Includes all systems in the database that have an operating system equal to Microsoft Windows 95, 98, or ME

- **HP Tru64 UNIX.** Includes all systems in the database that have an operating system equal to HP True64 UNIX
- **HP OpenVMS.** Includes all systems in the database that have an operating system equal to HP OpenVMS
- **Red Hat Linux.** Includes all systems in the database that have an operating system equal to Red Hat Linux
- **SuSE Linux.** Includes all systems in the database that have an operating system equal to SuSE Linux
- **Linux.** Includes all systems in the database that have an operating system equal to Linux
- **HP NonStop Server.** Includes all systems in the database that have an operating system equal to HP NonStop Server
- **Undeployed.** Includes all systems in the database that have an operating system equal to Undeployed

The following collections are based on Clusters by Type:

- **All Clusters.** Includes all cluster in the database
- **MSCS Clusters.** Includes all MSCS clusters in the database
- **OpenVMS Clusters.** Includes all OpenVMS clusters in the database
- **HP TruClusters.** Includes all HP TruClusters in the database
- **HP Serviceguard.** Includes all HP Serviceguard clusters in the database

The following default collections are based on Clusters by Status:

- **Critical Clusters.** Includes all clusters in the database with a Critical status
- **Major Clusters.** Includes all clusters in the database with a Major status
- **Minor Clusters.** Includes all clusters in the database with a Minor status
- **Normal Clusters.** Includes all clusters in the database with a Normal status
- **Unknown Clusters.** Includes all clusters in the database with an Unknown status

The following are System Function collections:

- **Data Collection List.** Includes all discovered systems and is used to perform data collection
- **Status Polling List.** Includes all discovered systems and their current status
- **Server Status Polling List.** Includes all discovered servers, clusters, management processors, and their current statuses
- **Non Server Status Polling List.** Includes all discovered non-servers and their current statuses

The following collection is added if HP Storage Essentials installed:

- **Storage Essentials Managed.** Includes all storage systems that are managed by HP Storage Essentials.

Shared Event Collections

All users can view shared event collections, but only users with full-configuration-rights can create, edit, or delete shared collections.

The following shared **Events** are based on Event by Severity:

- **All Events.** Includes all events that have occurred on systems for which the events are logged in the database
- **Important Events.** Includes all Critical and Major events in the database, regardless of the state of events
- **Important Uncleared Events.** Includes all uncleared Critical, Major, and In Progress events
- **Informational Events.** Includes all Informational events in the database, regardless of the state of events

The following are Login Event collections:

- **All Login and Logout Events.** Users with full-configuration-rights and users with the correct authorizations on the central management server (CMS) can view login and logout events. However, only users with full-configuration-rights can see the details of these events.
- **All Failed Login Events.** Users with full-configuration-rights and users with the correct authorizations on the CMS can view failed login events. However, only the users with full-configuration-rights can see the details of these events.

The following are Service Event collections:

- **All HP Service Events.** Includes all service events in the database where the event type is HP Service Events

Note: A service event indicates that a service action is required, such as hardware maintenance. You can open the service event to review the recommended actions and call status, if applicable.

Note: Service events can be obtained from HP Instant Support Enterprise Edition (ISEE) and Open Service Event Manager (OSEM). Go to <http://h18023.www1.hp.com/support/svctools/> and refer to the documentation for ISEE and OSEM and the *How to change the HP SIM Host Name* to configure these tools to send service events to HP Systems Insight Manager (HP SIM). In addition, a services contract might be required to receive these events.

The following collection is added if HP Storage Essentials installed:

- **Storage Essentials.** Includes all HP Storage Essentials events.

Related Procedures

- Customizing System or Cluster Collections
- Customizing Event Collections

Related Topics

- Navigating the Systems and Events Panel
- System Table View Page
- Event Table View Page
- Cluster Table View Page
- System Types
- Service Notification Events
- Changes to HP Systems Insight Manager Storage Functionality when HP Storage Essentials is Installed

Collection Naming Conventions

Use the following guidelines for naming **Systems** or **Events**:

- All collection names must be unique, except for private collection.
- The terms **Systems**, **Events**, and all shared collections are reserved names in HP Systems Insight Manager (HP SIM). Do not use them as collection names.
- Multiple spaces in collection names are collapsed to a single space. For example, a collection named,

My Collection, is saved as **My Collection**

- Do not use the following symbols in collection names: < > " & ' _ + | % \ / and ;
- After saving the collection, the name appears under the **Systems and Events** panel. All collection names must be unique.
- Private collection names cannot match the name of any **Systems** or shared collection but can match the name of a second users private collection.
- If you create a private collection and get a duplicate name error, you might find that the name exists in another users private collection.

Related Topics

- Monitoring Systems, Clusters, and Events
- Event Table View Page
- System Table View Page
- Cluster Table View Page
- Reference

Storage Integration

HP Systems Insight Manager (HP SIM) discovers SNMP and SMI-S storage devices.

- For information about using storage devices with HP SIM, refer to “Storage Integration Using SNMP” and “Storage Integration Using SMI-S”.
- For information about the configuration steps for discovering storage devices, refer to “Discovering Storage Using SNMP” and “About Storage Discovery Using SNMP” for SNMP devices and “Configuring HP Systems Insight Manager with Storage Systems” for SMI-S devices.

Related Topics

- Viewing Storage Systems
- Viewing Storage System Reports
- Viewing Storage Array Capacity
- Changes to HP Systems Insight Manager Storage Functionality when HP Storage Essentials is Installed
- Using HP Systems Insight Manager with SNMP Storage Solutions

Storage Integration Using SMI-S

About Storage Systems

Storage systems are SAN-attached Fibre Channel disk arrays, switches, tape libraries, or hosts (with Fibre Channel host bus adapters). HP Systems Insight Manager (HP SIM) uses WBEM SMI-S providers to discover and collect data from storage systems. Go to <http://www.hp.com/go/hpsim/providers> to view the latest information about HP SIM device support and for information on obtaining and installing SMI-S providers.

The default collection **Storage Systems** is listed under **Systems by Type** in the tree in the **Systems and Events** panel. The following collections are available under **Storage Systems**:

- **All Storage Systems.** This category includes all devices that were discovered through an SMI-S provider.
- **All Storage Hosts.** A storage host is a server, desktop, or workstation that is connected by a host bus adapter (HBA) to a storage area network (SAN). Storage hosts are also included in the **All Servers** and **All Systems** collections.
- **All Storage Switches.** A storage switch is a Fibre Channel switch that is connected to a SAN. Storage switches are also included in the **All Systems** and **All Network Devices** collections.
- **All Storage Arrays.** A storage array is a disk array that uses a Fibre Channel controller to connect to a SAN. Storage arrays are also included in the **All Systems** collection.
- **All Tape Libraries.** A tape library is a tape drive that is connected to SAN. Tape libraries are also included in the **All Systems** collection.

Related Procedures

- Configuring HP Systems Insight Manager with Storage Systems
- Viewing Storage System Reports
- Viewing Storage Systems
- Viewing Storage Array Capacity

Related Topics

- Changes to HP Systems Insight Manager Storage Functionality when HP Storage Essentials is Installed

Configuring HP Systems Insight Manager with Storage Systems

Configuring HP Systems Insight Manager with Storage Systems

For optimal interaction between HP SIM and storage systems, complete the following procedures.

Configure HP SIM to discover storage systems

HP Systems Insight Manager (HP SIM) discovers and identifies storage systems.

To discover and collect data from a storage system:

1. Verify that the storage system has an installed and configured SMI-S provider. Refer to the HP Systems Insight Manager Installation and User Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information about obtaining and installing SMI-S providers.
2. Enter the user name and password for the SMI CIMOM in the **Default WBEM settings** section on the “Setting Global Protocols” page.
3. Add each SMI CIMOM IP address to the **System Automatic Discovery** task, or create a new discovery task. Refer to “Editing a Discovery Task” and “Creating a New Discovery Task” for instructions.

Your storage systems will be discovered after the next automatic discovery task. If you want to discover your storage systems immediately, run the discovery task. Refer to “Running a Discovery Task” for instructions.

Subscribe to WBEM indication events

If a storage system's SMI-S provider supports WBEM indication events, and you want to view WBEM indication events on the Event View Page, you must subscribe to WBEM events for the storage system. Refer to “Subscribing to WBEM Indications” for instructions.

Related Procedures

- Setting Global Protocols
- Subscribing to WBEM Indications
- Editing a Discovery Task

- Running a Discovery Task
- Creating a New Discovery Task
- Viewing Storage Systems
- Viewing Storage System Reports

Related Topic

- Storage Integration Using SMI-S

Viewing Storage Systems

HP Systems Insight Manager allows you to view storage system information for collections and individual storage systems.

Viewing Storage System Collections

To view a storage system collection:

1. In the Systems and Events panel, expand **Systems, Shared, Systems by Type, and Storage Systems**.
2. Select one of the following:
 - **All Storage Systems**
 - **All Storage Hosts**
 - **All Storage Switches**
 - **All Storage Arrays**
 - **All Tape Libraries**

The system table view page for that collection appears. Refer to “Navigating the System Table View Page” for more information.

Viewing Individual Storage Systems

To view an individual storage system:

1. In the Systems and Events panel, expand **Systems, Shared, Systems by Type, and Storage Systems**.
2. Expand the storage system collection that contains the system you want to view.
3. Click the name of the storage system you want to view.

The System Page for that system appears. For more information, refer to “System Page”

Related Procedures

- Configuring HP Systems Insight Manager with Storage Systems
- Viewing Storage System Reports
- Viewing Storage Array Capacity

Related Topics

- Navigating the Systems and Events Panel
- Storage Integration Using SMI-S

Viewing Storage System Reports

HP Systems Insight Manager (HP SIM) provides predefined and customized storage system reports.

If HP Storage Essentials is installed, No data is displayed in HP SIM storage system reports. This is because HP SIM data collection from SMI-S devices is disabled to avoid duplicate data collection from both HP SIM and HP Storage Essentials. For information on storage system reporting with HP Storage Essentials, refer to your HP Storage Essentials documentation.

Refer to “Reporting Views” for specific details about the fields that are displayed in storage system reports.

Existing Storage System Reports

The following predefined reports are available:

- **Storage Device Capacity—All Storage Arrays** lists capacity usage details for all storage arrays.
- **Storage Device Controllers—All Storage Arrays** lists the status, port count, and number of ports utilized for each storage array controller.
- **Storage Device Inventory—All Storage Arrays** lists vendor, status, and port information for each storage array.
- **Storage Device Inventory—All Storage Hosts** lists vendor, status, and port information for each storage host.
- **Storage Device Inventory—All Storage Switches** lists vendor, status, and port information for each storage switch.
- **Storage HBAs—All Storage Hosts** lists vendor, status, and port information for each host bus adapter (HBA) that is installed on a storage host.
- **Storage Logical Units—All Storage Arrays** lists LUN information and status for all LUNs on all storage arrays.
- **Storage Ports—All Storage Arrays** lists port information for all storage arrays.
- **Storage Ports—All Storage Hosts** lists port information for all storage host HBAs.
- **Storage Ports—All Storage Switches** lists port information for all storage switches.

Note:



Refer to “System Reporting” for instructions on viewing existing reports.

Custom Reports

Refer to “Adding a Report” for instructions on creating custom reports.

Related Procedures

- System Reporting
- Adding a Report

Related Topics

- Reporting
- Storage Integration Using SMI-S
- Printing Reports
- Reference Information
- Reporting Views

Viewing Storage Array Capacity

HP Systems Insight Manager allows you to view capacity details for storage arrays.

Viewing Storage Capacity for All Arrays

To view storage capacity for all arrays, run the **Storage Device Capacity-All Storage Arrays** report. Refer to “System Reporting” for instructions.

Viewing Storage Capacity for a Single Array

1. In the **Systems and Events** panel, expand **Systems, Shared, Systems by Type, Storage Systems, and All Storage Arrays**.
2. Select a storage array.
3. Click the  next to **Capacity Information**.

Related Procedure

- Viewing Storage System Reports
- Viewing Storage Systems

Related Topics

- Storage Integration Using SMI-S
- Identity Tab for a Storage Array

Changes to HP Systems Insight Manager Storage Functionality when HP Storage Essentials is Installed

If HP Storage Essentials is installed, the following changes occur within HP Systems Insight Manager:

- HP Storage Essentials items are added to the **Tools, Deploy, Diagnose, Optimize, Reports, Tasks & Logs,** and **Options** menus. Refer to your HP Storage Essentials documentation for details about these menu items.
- A shared collection called **Storage Essentials Systems** is added to the **Systems & Events** panel.
- The following collections are included under **Storage Essentials Systems: All SE Systems, SE Servers, SE Switches, SE Storage Arrays, SE Tape Libraries,** and **SE Cluster Nodes.**
- If a storage system is managed by HP Storage Essentials, storage-specific details do not appear in its identity tab, and an **SE System Properties** link appears in the **HP Storage Essentials Pages** section on the **Tools & Links** tab. Click the **SE System Properties** link to view the Storage Essentials device page for this storage system.
- For storage hosts, HP Storage Essentials adds the **System Application Discovery Settings** link to the **Tools & Links Page.** Use this link to access the preferences for HP Storage Essentials system application discovery.
- No data is displayed in HP Systems Insight Manager storage system reports. This is because HP Systems Insight Manager (HP SIM) data collection from SMI-S devices is disabled to avoid duplicate data collection from both HP SIM and HP Storage Essentials. For information on storage system reporting with HP Storage Essentials, see your HP Storage Essentials documentation.
- The storage tables in HP SIM's Data Collection reports are not populated with data because HP SIM's SMI-S data collection is disabled.
- Storage systems that are managed by HP Storage Essentials show a subtype of **Storage Essentials Managed,** and do not show the **SMI** subtype.
- HP SIM determines device health status by polling the SMI-S providers of storage systems. If HP Storage Essentials discovered a storage array, storage switch, or tape library by a method other than SMI-S, HP SIM lists the device's status as **Unknown.**
- System properties that are edited in HP SIM are not transferred to HP Storage Essentials.
- The Suspend or Resume Monitoring command has no effect on HP Storage Essentials systems.
- HP Storage Essentials events are handled as follows:
 - HP Storage Essentials events are available in the **Events** tab of the **System Page** for all storage systems.
 - A collection called **Storage Essentials** is added to the list of shared collections under **Events** in the **Systems and Events** panel.
 - When an event is cleared in HP SIM, it is also cleared in HP Storage Essentials.
 - Deleting an event in HP SIM does not cause the event to be deleted in HP Storage Essentials.

- When an event is cleared in HP Storage Essentials, it is also cleared in HP SIM.
 - Deleting an event in HP Storage Essentials does not cause the event to be deleted in HP SIM.
 - Comments that are added to events in HP SIM are not transferred to HP Storage Essentials.
 - A link in the **Event Details** section allows you to view the corresponding event details in HP Storage Essentials.
-
- The **Automatic** tab on the **Discovery** page shows the status of the HP Storage Essentials discovery process and provides a link to the HP Storage Essentials discovery log.
 - The **General Settings** section in the **Automatic** tab on the **Discovery** page includes a link to the HP Storage Essentials global application settings configuration page.
 - When HP Storage Essentials is installed, a Toolbox for Storage Essentials tools is added to the **Toolboxes** tab of the **Users and Authorizations** page.

Note:



For additional information about HP Storage Essentials, see your HP Storage Essentials documentation.

Related Topics

- Storage Integration Using SMI-S
- HP Storage Essentials Overview

Storage Integration Using SNMP

Overview

Storage devices can be broken down into real-time access and back up systems. Real-time access systems can be subdivided into internal disks, redundant disks (RAID), tape libraries, storage area networks (SAN), and network attached storage (NAS).

Most data centers have combinations of these systems including:

- **Small Business.** Almost entirely internal disk drives
- **Medium Business.** Varying combination of internal disks and RAID systems
- **Large Business.** Varying combination of internal disks, RAID, and some SAN or NAS
- **Enterprise Business.** Mostly large SAN or NAS, and some RAID and internal disks might be present

HP Systems Insight Manager (HP SIM) can retrieve the information for the internal disk drives for systems being monitored. This does not mean that HP SIM actively manages and configures each of the systems previously indicated.

HP SIM can:

- Discover and identify storage systems that are directly attached to a server
- Discover and identify storage systems that are on the network, including tape libraries
- Discover and identify HP StorageWorks Command View storage device manager systems
- Receive storage system events and associate them with the system that generated the event (through Command View) running on a system, or from a tape library management card
- Context launch appropriate management application from the context of the event or the context of the system running the Command View that generated the event

Storage Events

HP SIM enables administrators to monitor inventory and, configure and manage hardware resources and the system software that affects the systems.

HP SIM provides the administrator with a complete overview of the hardware status. Storage events provide notification that a problem exists that could affect the availability of storage resources, which can affect system and application availability. HP SIM receives detailed event messages through WBEM events or SNMP traps. These events identify the system and the affected disk and provides an error number for looking up details and a description of the problem. The event details also contain links to the Command View server that generated the event. HP SIM associates a disk or RAID subsystem with the controller managing these drives for internal storage.

Storage Inventory Details

HP SIM inventory retrieves and stores the following information from internal disk drives:

- Disk
 - Total number of disk slots
 - Number of used slots
 - Slot ID
 - The type of disk in slot
 - Disk manufacturer
 - Disk model
 - Disk part number
 - Disk characteristics
 - Firmware version
 - Controller ID that is managing this disk

- Controller details
 - Total number of controllers
 - Controller type
 - Controller manufacturer
 - Model number
 - Part number
 - Slot ID in that this card is installed in
 - Firmware version
 - Controller characteristics

- RAID details
 - RAID type
 - RAID configuration

- SAN and NAS
 - Network addresses
 - Manufacturer
 - Model

- IS and MNHA
 - Part number
 - Total number of disks
 - Disk details
 - Servers being serviced by this system

Related Procedures

- Discovering Storage Using SNMP
- Using HP Systems Insight Manager with SNMP Storage Solutions

Related Topics

- System Page
- About Storage Discovery Using SNMP
- System Page

About Storage Discovery Using SNMP

Discovery and Identification

HP Systems Insight Manager (HP SIM) discovers the storage systems that are on the LAN and Command View storage device managers running on managed systems or devices. For internal disks, the HP SIM inventory component can identify all of the drives installed, the disk manufacturer, models, disk types, firmware revision, the internal location of the drive in the system, and the details of the controllers by which the systems are managed. For RAID drives, the RAID type (1 to 5) and manufacturer is discovered in addition to the details gathered for the internal drives. For SAN systems, HP SIM discovers the Command View servers that manage the devices on the SAN.

HP SIM displays storage systems as follows:

- **Internal drives.** These systems must appear in the **Properties** pages and the inventory database as components of their respective systems.
- **Tape libraries.** These devices are identified and included in the **All Systems, All Storage Systems,** and **All Tape Libraries** collections.
- **SAN.** The Command View systems for these devices are identified and available from the **Tools & Links** tab of the **System Page** for the systems serving the Command View systems.

Note:



HP SIM discovers SAN and NAS management applications and provides user access to system information on launch of those applications.

Related Procedures

- Discovering Storage Using SNMP
- Using HP Systems Insight Manager with SNMP Storage Solutions

Related Topic

- System Page

Discovering Storage Using SNMP

The HP Systems Insight Manager (HP SIM) discovery process for systems running Command View includes the following:

Note:



To access the links to Command View, select **Tools->System Information->System Page->Links**.

- CV XP on port 80 (http)
- CV VA/SDM on port 4096 (http)
- CV TL on port 4095 (http)
- Discovery of Command View EVA is encapsulated within the discovery of the HP StorageWorks Storage Management Appliance on ports 2301 or 2381

HP SIM must be permitted to access the Web server.

To configure Command View and SDM:

1. Verify that the HP Systems Insight Manager CMS is within a secure IP range in the Command View server configuration.
 - **Host based.** CMS IP address included in
.../sanmgr/hostagent/config/access.dat.
 - **Storage Area Manager management server (if applicable).** CMS station IP address included in
/sanmgr/managementserver/config/authorizedClients.dat.
2. Run Discovery to discover or re-identify the Command View systems. Refer to "Discovery and Identification" for more information regarding running discovery.
3. When discovery is complete, you can group systems in HP SIM and launch Command View from the **System Page**. Refer to "System Page" for more information regarding the **System Page**.

To load the EVA MIB, enter `mxmib -a cpqhsv110v3.cfg`.

Note: Loading the MIB could take several minutes to complete. Refer to "Managing MIBs" for more information about MIBs.

Related Procedure

- Using HP Systems Insight Manager with SNMP Storage Solutions

Related Topics

- System Page
- About Storage Discovery Using SNMP
- Discovery and Identification

Using HP Systems Insight Manager with SNMP Storage Solutions

Viewing a Storage Event

There are two ways to view a storage event:

- Select **Tools>System Information>System Page**.

- Click the system name in the **System Name** column on the system table view page.

Creating a Storage by Type Group

You can create a search for systems of type, such as ESL or MSL, for tape libraries, or create a search for Web Agents of type for each type of Command View system.

- **HP StorageWorks Command View SDM.** Search for Web Agent == HP StorageWorks Command View SDM.
- **HP StorageWorks Command View XP.** Search for Web Agent == HP StorageWorks Command View xp.
- **HP StorageWorks Command View ESL.** Search for Web Agent == HP StorageWorks Command View ESL.
- **HP StorageWorks Tape Libraries.** Search for system type == storage device.
- **HP StorageWorks Management Appliance.** Search for Web Agent == Management module hp_OpenView_Storage_Management_Appliance or Web Agent == Management Module OpenSANManager.

Event Collection and Launch

To receive events, the Command View software must be configured to send SNMP events to the HP Systems Insight Manager (HP SIM) CMS.

For Command View SDM:

To configure the SNMP trap destination on Windows NT 4.0 on the Command View server:

1. Select **Start->Settings->Control Panel->Network->Services->SNMP Service**.

The **SNMP Service Properties** dialog box appears.

2. Click **Traps**.
3. Enter a community name, such as **public**.
4. Click **Add**.
5. At the bottom of the dialog box, click **Add**.

The **SNMP Service Configuration** dialog box appears.

6. Enter the hostname or IP address of the enterprise management station, and click **Add**.

The SNMP trap destination is added.

7. Click **OK** to save the changes and close the dialog box.

To configure the SNMP trap destination on Windows 2000:

1. Click **Start->Settings->Control Panel->Network->Services->SNMP Service**.

The **SNMP Service Properties** dialog box appears.

2. Click **Traps**.
3. Enter a community name, such as **public**.
4. Click **Add to list**.
5. At the bottom of the dialog box, click **Add**.

The **SNMP Service Configuration** dialog box appears.

6. Enter the hostname or IP address of the enterprise management station, and click **Add**.

The SNMP trap destination is added.

7. Click **OK** to save the changes and close the dialog box.

To configure the SNMP trap destination on HP-UX:

1. Using a text editor, open the following file:

```
/etc/snmpd.conf
```

2. Insert the following information at the end of the `snmpd.conf` file:

```
trap-dest: X.X.X.X
```

Replace the `X.X.X.X` with the IP address of the enterprise management station.

3. Save and close the `snmpd.conf` file.
4. Kill the SNMP daemon by entering the following at a shell command prompt:

```
ps -ef | grep snmpd
```

```
kill -9 PID
```

Replace `PID` with the process ID returned by the previous command.

5. Restart the SNMP daemon by entering the following at a shell command prompt:

```
snmpd
```

To load the HSV MIB on the CMS for EVA:

1. On a Windows operating system go to a command prompt. Navigate to `\Program Files\HP\System Insight manager\mibs` directory. Refer to "Registering a MIB" for more information regarding MIBs.
2. Run `mxmib -a cpqhsv110v3.cfg`.

Related Procedures

- Discovering Storage Using SNMP
- Configuring SNMP Traps

Related Topics

- [System Page](#)

Managing with Tasks

HP Systems Insight Manager (HP SIM) enables you to manage systems and events by scheduling and executing tasks. Tasks are actions performed using an HP SIM tool. Task instances are an executed single instance of a task.

Users can:

- Create their own variation of a task
- Schedule a task
- Modify a task they created
- Delete a task
- Stop an executing task
- Track task status

Task information is available by selecting:

- **Tasks & Logs->View All Scheduled Tasks**

or

- **Tasks & Logs->View Task Results**

User Privileges

The list of tasks that a user can see are based on the user's privilege and access level. All users are allowed to edit, delete, and view the tasks they created. A user with full-configuration-rights is allowed to edit, delete, and view tasks other users created.

Note:



HP SIM provides some system delivered tasks or default tasks. These tasks can be disabled or have their schedules modified but cannot be removed or reassigned to another user. HP SIM requires these tasks to provide a complete picture of the systems that are being monitored.

Related Procedures

- Creating a Task
- Scheduling a Task
- Running a Scheduled Task
- Stopping a Task
- Deleting Task Results
- Printing Reports
- Editing a Scheduled Task

- Deleting a Scheduled Task
- Viewing Task Results

Related Topics

- About Default Polling Tasks
- Navigating the All Scheduled Tasks Page
- Applying a Time Filter
- Task Status Types

About Default Polling Tasks

Polling tasks track health status for systems in the associated collections. Hardware Status Polling needs to occur periodically in order to determine when systems go offline or hardware degrades. You can customize polling tasks for specific systems to run at scheduled times. You can also create new polling tasks with different collections to match your specific requirements.

Data Collection Tasks are included with other polling tasks. Data Collection finds more specific system information, such as asset data.

You can configure the polling tasks to take place based on the receipt of an event. Event Polling Tasks are associated with event collections. For example, you might set up a Hardware status polling task for when traps are received from a system.

When a polling task is set up to run as the result of a change in an event collection, the polling task is applied to all systems generating events that match the given collection.

Note:



It is not advisable to schedule a polling task based on an event collection periodically. The task would run on the set of systems for each event in the associated collection.

Note:



Do not delete or disable default tasks without replacing them with a substitute task that achieves a similar result. For example, if you remove a hardware status polling task, systems continue to be discovered, but status on them is not updated. If you remove the Daily Device Identification task, you would no longer detect any changes in management on systems.

The following default polling tasks are available on the **View All Scheduled Tasks** page:

- Bi Weekly Data Collection
- Daily Device Identification
- Hardware Status Polling for non Servers

- Hardware Status Polling for Servers
- Hardware Status Polling for Systems no Longer Disabled
- Initial Data Collection
- Initial Hardware Status Polling
- Software Version Status Polling
- Software Version Status Polling for Systems no Longer Disabled

Bi Weekly Data Collection

The Bi Weekly Data Collection task runs on all of the systems in the **Data Collection List** collection. The default schedule is to run every other Saturday at noon.

Daily Device Identification

Use the Daily Device Identification task to identify information about systems like networking systems. This task runs once a day by default and the information is stored in the database. The following information is identified:

- Determines Single Login and Secure Task Execution (STE) support on a managed system
- Type of management protocol on the system (HTTP, SNMP, DMI, WBEM)
- Type and subtype of system (server, storage, switch, router, and so on)
- Product name of the system
- Operating system name and version
- Web Agents running on the system
- Web-based software running on the system, for example, printer management software
- System associations with management processors, for example, a system and its Remove Insight Board
- Storage proxies and related storage systems
- Wake-on-LAN information

Hardware Status Polling for non Servers

This task collects status information through management protocols (SNMP, WBEM, and so on) for systems that are not of a Server, Cluster, or Management Processor type. This task is configured to poll every 10 minutes and at startup by default.

Note:



If you discover more than 500 systems, HP suggests you change the interval to something greater than 10 minutes. For example, 15 minutes for every 1000 systems.

Hardware Status Polling for Servers

This task collects status information for SNMP systems of type Server, Cluster, or Management Processor. This task is configured to poll every five minutes and at startup by default.

Note:



If you discover more than 500 systems, HP suggests you change the interval to something greater than 5 minutes. For example, 10 minutes for every 1000 systems.

Hardware Status Polling for Systems no Longer Disabled

This task runs when a system goes from a disabled state to an enabled state. You could use this task to get the latest status after a planned maintenance window on a system that was set to disabled..

Initial Data Collection

This task collects *static* information from a number of systems that have WBEM, DMI, or SNMP running. For example, serial numbers and model numbers. This task is set to run by default when a new system matches the data collection. For more information on what data is collected, refer to "Reference Information".

Initial Hardware Status Polling

This task runs hardware status polling on systems that are newly discovered. Therefore, you do not need to wait for the periodic tasks to run before the system has a valid status..

Software Version Status Polling

This task determines software version update status and is set to run every seven days, on Wednesday at Midnight, but default. You can edit this task or manually run it at any time.

Refer to "Software Status Polling" for more information.

Software Version Status Polling for Systems no Longer Disabled

This task runs the software version tool when a system goes from a disabled state to an enabled state, so that the status of the software loaded on the system is kept up to date in HP Systems Insight Manager (HP SIM).

Refer to “Software Status Polling” for more information.

Related Procedures

- Creating a Task
- Running a Scheduled Task
- Editing a Scheduled Task
- Printing Reports
- Running a Scheduled Task
- Editing a Scheduled Task

Related Topic

- Navigating the All Scheduled Tasks Page

Creating a Task

Create a task to execute a tool on specific systems or events.

Note:



If multiple users are accessing a task simultaneously, the changes from the last user to edit the task are saved. For example, if User1 and User2 sign into HP Systems Insight Manager (HP SIM) with full-configuration-rights and User1 is editing a task while User2 is deleting the same task, then when User1 tries to save the edited task, a message appears, indicating that the task does not represent an object in the system. User1 is unable to save the edited task.

To create a task:

1. Select a tool from the menu. The **Select Target Systems** page appears.

Note: The **Verify Target Systems** page appears if targets are selected before selecting a tool.

2. To add targets, select a group from the dropdown list. The contents of the selected group appear and can be selected as targets or to select the collection itself, select **Select Name of Collection itself**.

Note: Selecting **Select "collection" itself** results in better performance overall when running the task on all systems in the collection.

3. Click **Apply**. The targets appear in the **Verify Target Systems** section.

Note: If any selected targets are not compatible with the tool, the **Tool Launch OK?** column provides a brief explanation of the problem. To remove a target, select the target's checkbox and then click **Remove Targets**.

4. Select one of the following options:
 - Click **Add Targets** to add more targets to the **Target System List**.
 - To remove a target, select the target's checkbox and then click **Remove Targets**.
 - Click **Next** to specify tool parameters and to schedule the task.
5. Specify tool parameters. If the tool does not require any parameters, **Next** is replaced with **Schedule** and **Run Now** buttons. The **Schedule** option is only present if the tool can be scheduled.
6. Select one of the following options:
 - Click **Previous** to return to the previous screen.
 - Click **Schedule** to schedule when the task should run. Refer to "Scheduling a Task" for more information about scheduling options.
 - Click **Run Now** to run the task immediately.

Command Line Interface

Use the **mxexec** command to execute tools immediately and the **mxtask** command to schedule tasks for later. Perform this task from the command line interface (CLI). For assistance with this command, refer to the HP-UX or Linux manpage by entering **man mxexec** at the command line or refer to the Windows command line help. Refer to "Using Command Line Interface Commands" for information on accessing the manpage.

Default Tools

- **Cluster Monitor.** Refer to "Cluster Monitor" for more information.
- **Collect Keys.** Refer to "Collecting Keys" for more information.
- **Command Line Tools.** Refer to "Command Line Tools" for more information.
- **Data Collection.** Refer to "Data Collection" for more information.
- **Delete Events.** This tool is used to delete events from a specific event collection.
- **Deploy Keys.** Refer to "Deploying Keys" for more information.
- **Device Ping.** Refer to "Device Ping" for more information.
- **Disk Thresholds, Setting.** Refer to "Setting Disk Thresholds" for more information.
- **DMI Access, Configuring.** Refer to "Configuring DMI Access" for more information.

- **Hardware Status Polling.** Collect hardware status based on the protocols supported on the target system.
- **Identify Systems.** Refer to “Identification” for more information.
- **Initial ProLiant Support Pack Install.** Refer to “Initial ProLiant Support Pack Install” for more information.
- **Install Software and Firmware.** Refer to “Installing Software and Firmware” for more information.
- **Manage Keys.** Refer to “Managing Keys” for more information.
- **Management Information Base (MIB), Managing.** Refer to “Managing MIBs” for more information.
- **Management Processor Tools.** Refer to “Management Processor Tools” for more information.
- **OpenSSH, Installing and Deploying.** Refer to “Deploying OpenSSH to Multiple Systems Using RDP” for more information.
- **Performance Management Pack (PMP) Tools.** Refer to “PMP Tools” for more information.
- **Program/Script Launches.** Refer to “Custom Commands” for more information.
- **Property Pages.** Refer to “Property Pages” for more information.
- **Replicate Agent Settings.** Refer to “Creating a Replicate Agent Settings Task” for more information.
- **Reporting Snapshot.** Refer to “Snapshot Comparison Reporting” for more information.
- **RPM Package Manager Tools.** Refer to “RPM Package Manager” for more information.
- **Server Migration Pack.** Refer to “Server Migration Pack” for more information.
- **System Protocol Settings.** Refer to “Setting Protocols for a System or Groups of Systems” for more information.
- **SNMP Access, Configuring.** Refer to “Configuring SNMP Access” for more information.
- **Software Status Polling.** Refer to “Software Status Polling” for more information.
- **Storage Solutions Integration.** Refer to “Storage Integration Using SNMP” for more information.
- **System Management Homepage.** Refer to “System Management Homepage” for more information.
- **System Page.** Refer to “System Page” for more information.
- **System Properties, Setting.** Refer to “System Properties” for more information.
- **Version Control Agent.** Refer to “Accessing the Version Control Agent” and “Accessing the Version Control Repository Manager” for more information.

- **Virtual Machine Management Pack (VMM).** Refer to “Virtual Machine Management Pack ” for more information.
- **Webmin.** Refer to “Webmin Overview” for more information.

Related Topics

- Managing with Tasks
- Navigating the All Scheduled Tasks Page

Navigating the All Scheduled Tasks Page

The **All Scheduled Tasks** page displays the tasks that are scheduled to run at periodic times or based on events criteria. A scheduled task can also have a schedule of **not scheduled**, which means that the task is listed but only runs when manually executed by a user.

Task information is available by selecting **Tasks & Logs->View All Scheduled Tasks**. Select a task by clicking the task row. Refer to:

- “Run Now”
- “Edit”
- “Delete”
- “View Task Results”

Note:



If multiple users are accessing a task simultaneously, the changes from the last user to edit the task are saved. For example, if User1 and User2 sign into HP Systems Insight Manager (HP SIM) with full-configuration-rights and User1 is editing a task while User2 is deleting the same task, then when User1 tries to save the edited task a message appears, indicating that the task does not represent an object in the system. User1 is unable to save the edited task.

User Privileges

The list of tasks that a user can see are based on the user's privilege and access level. All users are allowed to edit, delete, and view the tasks they created. With full-configuration-rights, a user is allowed to edit, delete, and view tasks other users created.

Run Now

Run a task to initiate a task instance. Running a predefined task executes a specific tool on specific systems or events. Select **Tasks & Logs->View All Scheduled Tasks**. Select a task, and click **Run Now**. Refer to “Running a Scheduled Task” for more information.

Edit

Select the task to be edited. The previously configured task information appears. Use the same steps as if you are creating the task. Select **Tasks & Logs->View All Scheduled Tasks**. Select a task, and click **Edit**. Refer to “Editing a Scheduled Task” for more information.

Delete

Select the task to be deleted. Deleting a task removes the task from the **All Scheduled Tasks** page and the system. Deleting a task also deletes its associated task instances. Select **Tasks & Logs->View All Scheduled Tasks**. Select a task, and click **Delete**. Refer to “Deleting a Scheduled Task” for more information.

View Task Results

Select a task to view. The **Task Results** display below the **All Scheduled Tasks**. Information such as the tasks schedule, the tool used by the task, and the command the task executes is displayed. The **Task Results** also displays a list of the task instances created by the task. Below the task instances, the summary status, target systems list, and the target details are displayed.

Refer to “Viewing Task Results” for more information.

Related Topics

- Managing with Tasks
- Task Status Types

Scheduling a Task

The options presented for scheduling a task vary depending on the tool used and the type of target systems selected. Scheduling a task requires a unique name for the task. Not all tools can be scheduled.

To schedule a task:

1. Select a tool from the menus, and follow the steps to get to the **Schedule** button and click it. Refer to “Creating a Task” for more information.
2. In the **Task name** field, enter a unique name for the task.
3. Under **When would you like this task to run?** section, select one of the following options:
 - **Periodically**. Select from intervals of minutes, hours, days, weeks, or months. With periodic scheduling, the task can be configured to run until a certain date and time or to only execute a set number of times. Periodic scheduling allows time filters to be applied, which specifies at which hours of the day a scheduled task is allowed to operate. Refer to “Applying a Time Filter” for more information on time filters.
 - **Once**. Specify the date and time the task is to run.
 - **When new systems or events meet the list criteria**. This option is only available if you select a **List of Systems or Events** as your targets. The task runs only when new systems

or events meet the list criteria. You can also apply a time filter to this type of scheduling. Refer to “Applying a Time Filter” for more information on time filters.

- **When systems or events no longer meet the list criteria.** This option is almost identical to the previous option, except that the task only runs when the **List of Systems or Events** no longer meets the list criteria. A time filter can be applied to this type of scheduling. Refer to “Applying a Time Filter” for more information on time filters.
 - **Not Scheduled.** This option specifies that the task only runs when manually executed by a user with the appropriate privileges. This task never runs automatically. Tasks can be manually run from the **All Scheduled Tasks** page or the command line interface (CLI).
4. Under **In addition**, select from the following options:
- **Run when the central management server is started.** Select this option if you want the task to run when the central management server (CMS) is started.
 - **Run now.** Select this option to run the task immediately after it is saved.
 - **Disable this task.** Select this option to temporarily disable the task. This task is listed as Disabled on the **All Scheduled Tasks** page.
5. After a scheduling option has been selected, refine the schedule in the **Refine schedule** section. The available options vary depending on the scheduling option selected in step 3.
6. Click **Done** and the **All Scheduled Tasks** page appears, or click **Previous** to return to the previous page. Refer to “Navigating the All Scheduled Tasks Page” for more information on the **All Scheduled Tasks** page.

Viewing All Scheduled Tasks

To view all scheduled tasks, select **Tasks & Logs->View All Scheduled Tasks**.

The list of tasks that a user can see are based on the user's privilege and access level. All users are allowed to edit, delete, and view the tasks they created. With full-configuration-rights, the user is allowed to edit, delete, and view tasks other users created.

Related Procedures

- Running a Scheduled Task
- Viewing Task Results
- Deleting Task Results
- Printing Reports
- Editing a Scheduled Task

Related Topics

- Applying a Time Filter
- Managing with Tasks

Running a Scheduled Task

Run a task to initiate a task instance. Running a scheduled task executes a specific tool on specific systems or events.

To run a scheduled task:

1. From the tool menus, select **Tasks & Logs->View All Scheduled Tasks**. The **All Scheduled Tasks** are displayed in the workspace.
2. Select a task from the list, and click **Run Now**.

Note: If the task currently has a task instance running, the **Run Now** button is disabled.

Command Line Interface

Use the **mxexec** command to execute tools immediately and the **mxtask** command to schedule tasks for later. Perform these tasks from the command line interface (CLI). For assistance with this command, refer to the HP-UX or Linux manpage by entering **man mxexec** at the command line or refer to the Windows command line help. Refer to “Using Command Line Interface Commands” for more information on how to access the manpage.

Related Procedures

- Editing a Scheduled Task
- Deleting a Scheduled Task
- Printing Reports
- Viewing Task Results
- Stopping a Task

Related Topics

- Managing with Tasks
- Navigating the All Scheduled Tasks Page

Editing a Scheduled Task

Edit a scheduled task to change the tool parameters, set the time, re-enable a task that has been disabled, or modify target systems.

To edit a scheduled task:

1. Select **Tasks & Logs->View All Scheduled Tasks**. The **All Scheduled Tasks** page appears.
2. Select the task to be edited from the **All Scheduled Tasks** page.
3. Click **Edit**.

The previously configured task information appears. Follow the same steps as if you are creating the task. Refer to “Creating a Task” for more information.

Because the task has a schedule associated with it, you must visit the **Schedule Task Page**; the **Run Now** button is not present as it is when a new task is being created. Users with full-configuration-rights can also change the owner of the task.

If the new owner does not have access rights to the tool or one or more of the selected targets, an error message appears when the user attempts to edit or save the task.

4. After the task has been edited, click **Done**. This task is saved and displayed on the **All Scheduled Tasks** page.
5. To run the task immediately, select the **Run Now** checkbox on the **Schedule Task** page before clicking **Done**.

Related Procedures

- Running a Scheduled Task
- Deleting a Scheduled Task
- Printing Reports
- Viewing Task Results
- Stopping a Task

Related Topics

- Managing with Tasks
- Navigating the All Scheduled Tasks Page

Deleting a Scheduled Task

Deleting a task removes the task and its associated task instances from the **All Scheduled Tasks** page and the system.

Caution:



If you delete a task, the task is permanently deleted from the database and cannot be restored.

Note:



The system delivered, or default, tasks cannot be deleted.

To delete a scheduled task:

1. Select **Tasks & Logs->View All Scheduled Tasks**.
2. Select a task from the **All Scheduled Tasks** list.
3. Click **Delete**.

Note: If the task currently has a task instance running, a message appears, stating that you must stop the running task instance before the task can be deleted.

Related Topics

- Navigating the All Scheduled Tasks Page
- Scheduling a Task

Viewing Task Results

View **Task Results**, **Task Instance Results**, and **Target Details** to see a log of tasks performed on a system and the associated results. You can also print reports of task instances.

Viewing Task Results

The task results are displayed on the **Task Results** page. Information, such as the task start and stop time, the tool used by the task, and the command the task executes, are displayed.

1. Select **Tasks & Logs**->**View Task Results**.
2. To stop or delete a task instance, select a task instance from the **View Task Results** page.
3. Click **Stop** or **Delete**.

The **Task Results** page displays a list of the task instances created by all tasks.

Viewing Task Instance Results

From the **View Task Results** page, select a task instance by selecting a row from the Task Instances list.

The **Task Instance** section displays the following information:

- **Status**. This field displays the status of the task.
- **ID**. This field displays the task job ID number.
- **Task Name**. This field displays the name of the task that was executed.
- **Tool**. This field displays the name of the tool that was used.
- **Owner**. This field displays the user name that currently owns the task.
- **Command**. This field displays the command used to run the task.
- **Summary Status**. This field displays the summary status and indicates the status of the task for some tasks only. Refer to "Task Status Types" for more information.
- **Target**. This field displays the name of the target collection or individual systems against which the task executed. If you run a custom command or an multiple-system aware (MSA) tool, this field displays the central management server (CMS) system name. With MSA commands, the command resides on the CMS and is actually run from the CMS against a remote system or list of systems. Therefore, the target for this type of command always shows as the CMS.
- **Executed As**. This field displays the user context the tools was executed under.
- **Start Time**. This field displays the time when the task was started.

- **End Time.** This field displays the time when the task was completed or cancelled.
- **Duration.** This field displays the amount of time it took to run the task.

Note:



The list of task instances is based on user privileges and access levels. Users with full-configuration-rights can view all task instances known to the system.

Viewing Target Details

Note:



This section is displayed for single-system aware (SSA) tools only.

From the **Task Instance Results** section, select a target system from the table below the **Summary Status**.

The **Target Details** section displays the following information:

- **Status.** This field displays the status of the target.
- **Exit Code.** This field represents the success or failure of an executable program. Typically, if the return value is zero or positive, the executable ran successfully. If a negative value is returned, the executable failed.
- **Target Name.** This field displays the name of the target.
- **The Stdout Tab.** This tab displays the output text information.
- **The Stderr Tab.** This tab displays information if the executable experienced an error.
- **Files Copied Tab.** This tab displays what files are in the process of being copied or have been copied to the target system. This tab is not present for tools that do not perform any file copies to their target systems.

Viewing a Printable Report

Reports can be printed for the currently selected target system or for all target systems associated with the task instance.

To print a report:

1. Click **View Printable Report**.

An **Options Message** box appears, asking if you want to generate a report containing only the currently selected target system or all systems associated with the task instance. This option is only present if there is more than one target for the task instance.

2. Select which report to print.
3. Click **Print** to print the report, or close the window to return to the **View Task Results** page.

Related Procedures

- Running a Scheduled Task
- Deleting a Scheduled Task
- Printing Reports
- Editing a Scheduled Task
- Stopping a Task

Related Topics

- Managing with Tasks
- Navigating the All Scheduled Tasks Page

Printing Reports

Reports can be printed for the currently selected target system or all target systems associated with the task instance. For task instances that do not have multiple target systems, the report is created without asking whether you want to view the report for the currently selected target system or all target systems.

To print a report:

1. Select **Tasks & Logs->View Tasks Results**.
2. Click **View Printable Report**.

A **Print Report Question** appears, asking to generate a report containing only the currently selected target system or all target systems associated with the task instance.

3. Select which report to print.
4. Click **OK** to print the report.

Related Procedures

- Running a Scheduled Task
- Deleting a Scheduled Task
- Editing a Scheduled Task
- Viewing Task Results
- Stopping a Task

Related Topics

- Managing with Tasks
- Navigating the All Scheduled Tasks Page

Task Results List

The **Task Results** list displays the list of task instances known to the system. Each task instance listed displays its unique job ID, the name of the task, its owner, status, duration, and the start and end time for the task. The **Task Results** list lists status information from scheduled tasks that have run, as well as status information from runnable tasks, which are tasks that do not have a schedule. The **Task Results** list enables you to stop, delete, and view task instance results.

To see task information, select **Tasks & Logs->View Task Results**. Click the task row, and select one of the following options:

- **Stop**. Click **Stop** to stop a running task instance. Refer to “Stopping a Task” for more information.
- **Delete**. Select a task instance, and click **Delete**. Refer to “Deleting Task Results” for more information.

Note: If the task instance is currently running, a message appears, informing you to stop the task instance before attempting to delete it.

The results of a task instance are displayed below the **Task Results** list.

The **Task Instance Results** section displays the following information:

- **Status**. This field displays the status of the task. Refer to “Task Status Types” for more information on the different status types.
- **ID**. This field displays the task job ID number.
- **Task Name**. This field displays the name of the task that was executed.
- **Tool**. This field displays the name of the tool that was used.
- **Owner**. This field displays the user name that currently owns the task.
- **Command**. This field displays the command used to run the task.
- **Target**. This field displays the name of the target collection or individual systems against which the task executed. If you run a custom command or an multiple-system aware (MSA) tool, this field displays the central management server (CMS) system name. With MSA commands, the command resides on the CMS and is actually run from the CMS against a remote system or list of systems. Therefore, the target for this type of command always shows as the CMS.
- **Executed As**. This field displays the user context the tools was executed under.
- **Start time**. This field displays the time the task was started.
- **End time**. This field displays the time the task ended.
- **Duration**. This field displays the time that the task took to run.

The list of task instances is based on user privileges and access levels. Users with full-configuration-rights can view all task instances known to the system.

Related Topics

- Creating a Task
- Managing with Tasks

Stopping a Task

Perform this procedure to stop a task instance from running.

To stop a task instance:

1. Select **Tasks & Logs->View Task Results**, and select a task instance from the **Task Results** list.
2. Click **Stop**. If the task instance is in a terminal state, **Stop** is disabled. If the task can be stopped, a dialog appears, asking if you want to cancel or kill the selected task instance. If the tool does not signify that the task can be killed, the dialog box asks you to confirm the cancellation of the task instance. Killing a task attempts to interrupt any In Progress commands, while canceling stops Pending systems from starting and enables any Running or In Progress commands to complete.

Related Procedures

- Running a Scheduled Task
- Editing a Scheduled Task
- Deleting a Scheduled Task
- Printing Reports
- Viewing Task Results

Related Topics

- Scheduling a Task
- Task Results List
- Navigating the All Scheduled Tasks Page

Deleting Task Results

Perform this procedure to delete task instances from the **Task Results** page.

Note:



When a user is deleted from HP Systems Insight Manager (HP SIM), any tasks that belonged to that user are deleted as well.

To delete an instance:

1. Select **Tasks & Logs->View Task Results**.

Select a task from the table.

2. Click **Delete**. The task instance is deleted from the database.

Note: If the task instance is currently running, a message appears, stating that you must stop the running task instance before it can be deleted.

Command Line Interface

Use the **mxtask** command to execute tools immediately and to schedule tasks for later time. Perform this task from the command line interface (CLI). For assistance with this command, refer to the HP-UX or Linux manpage by entering **man mxtask** at the command line or refer to the Windows command line help. Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Procedures

- Creating a Task
- Stopping a Task

Related Topic

- Managing with Tasks

Applying a Time Filter

Use time filters to decide when a task should or should not run by applying them to a task. Time filters can be created, copied, edited, and deleted.

Time filters can be created by any user and are accessible to all users.

1. Select a tool from the tool menus and follow the steps to get to the **Schedule** button and click it. Refer to “Creating a Task” and “Scheduling a Task” for more information.
2. To apply a time filter to a task, select the **Use Time Filter** checkbox.
3. Click **Manage Filters**. The **Manage Time Filters** section appears below the **Schedule Task** section. Four options are available:
 - **New**. A new time filter can be created by clicking **New** from the **Manage Time Filter** box. The new time filter has the default name **New Time Filter X**, where X is a number making the time filter name unique. Click **OK** or **Apply** to save the new time filter, or click **Cancel** to cancel the new time filter changes.
 - **Edit**. Time filters created by users can be edited. A time filter cannot be renamed, so if a time filter must be renamed, copy the time filter first and then rename it. Changes made to a time filter are saved after clicking **OK** or **Apply**. If the time filter to be edited is in use by one or more tasks, a message displays, stating, *Editing the time filter could have undesirable effects in the tasks currently using the time filter.* To eliminate this problem, rename the time filter.

- **Copy.** Time filters may be copied by any user. The copied time filter displays and has a number X appended to the name of the time filter. X is a number making the time filter name unique. To save changes made to the time filter, click **OK** or **Apply**.
- **Delete.** A user can delete any time filter that is created by another user. Select the time filter to be deleted, and click **Delete**. If the time filter being deleted is in use by one or more tasks, a message displays, stating *The time filter cannot be deleted at this time because it is in use by one or more tasks.*

Time filters are created and viewed in the time zone of the user creating the time filter. For example, if the default time filter of business hours (8am to 5am) is used and the filter is viewed in the same time zone as the central management server (CMS), it will display from 8am to 5pm. If the CMS is in Eastern Standard Time (EST) and a user browses in from Pacific Standard Time (PST), the time filter appears as 5am to 2pm instead. Also, the time filters created on install use the time zone of the CMS.

Related Topics

- Managing with Tasks
- Scheduling a Task

Task Status Types

HP Systems Insight Manager (HP SIM) reports the following summary status for tasks:

-  **Failed.** The task instance has failed and needs immediate attention.
-  **Killed.** The task instance was stopped.
-  **Canceled.** The task instance was canceled before the task was complete.
-  **Complete.** The task instance is complete.
-  **Running.** The task instance is running without a problem.
-  **Copying.** The task instance is copying without a problem.
-  **Pending.** The task instance is not complete or is pending.
-  **Skipped.** The task instance includes a system that is not supported or the system was in a disabled state.

Note: When a tool does not support a system (for example, running a Windows tool on a Linux system), the task status is **Skipped** and the tool is not run on that system. The task is allowed to be created against collections even if some systems might not match the tool filter. When the task runs, the tool filtering is applied at that point. This differs from selecting a handful of systems in the UI and receiving the verify target selections screen with errors like `system is not a Linux OS`. Skipped is also displayed if a system is disabled and a polling tool (for example, Status polling or Data Collection) is run on it.

Related Topic

- Managing with Tasks

Tools that Extend Management

HP Systems Insight Manager (HP SIM) provides you with many powerful tools:

- **Cluster Monitor.** Adds the ability to monitor and manage multi-system MSCS clusters
- **Command Line Tools.** Command line tools are part of a distributed task facility (DTF) and one of the tools available in HP SIM to run on single-system aware (SSA) systems
- **Custom Commands.** Enables you to create and manage custom command tools that launch applications or scripts on the central management server (CMS) (not on target systems) and can reference environment variables set by the tool to access system or event information
- **Device Ping.** Enables you to ping one or more systems
- **Disk Thresholds.** Defines the Normal, Minor, and Major ranges for disk utilization on monitored nodes and is used to set and remove disk thresholds
- **DMI Access.** Allows setting the HP SIM central management server (CMS) as the event target on selected HP-UX systems where DMI has been installed
- **HP ProLiant Essentials Server Migration Pack (SMP).** Extends the functionality of the HP ProLiant Essentials Virtual Machine Management Pack (VMM) to provide integrated physical-to-virtual machine (P2V) and virtual-to-virtual machine (V2V) migrations
- **Initial ProLiant Support Pack Install.** Enables you to install software to managed systems
- **Licensing.** Provides the ability to manage license keys from HP SIM, including key distribution, reconciliation, and reporting across Windows platforms
- **Management Processor tools.** After management processors have been discovered, the following tools are available: system power, system locator, new user, modify user, delete user, LAN access, LDAP settings, iLO control, firmware update, and deploying SSH public keys
- **Management Information Base (MIB) tools.** The following tools are available for managing MIBs: compiling MIBs, editing MIBs, registering and unregistering MIBs, and viewing MIBs
- **OpenSSH Install.** Runs from the central management server (CMS) and installs the OpenSSH service onto target Windows systems and then runs the `mxagentconfig` command to complete the configuration
- **Performance Management Pack (PMP).** Enables you to watch and analyze in real-time the performance of a monitored server and view recorded data sessions directly from the PMP repository
- **Process Resource Manager (PRM) tools.** HP's Process Resource Manager (PRM) enables the system administrator to focus the appropriate amount of system resources exactly where the business needs them
- **Property Pages.** Enables a user with full-configuration-rights to view the **Property** pages on any WBEM system, including WBEM properties that help describe the target system on the network, WBEM properties that help determine the status of the system, and an inventory of the target system based on WBEM properties

- **Replicate Agent Settings.** Enables HP SIM to retrieve and optionally edit Web agent configuration settings from a source system and distribute that configuration remotely to one or more target systems through their Web agents
- **Serviceguard Clusters.** Provides a mechanism to view cluster information by running HP Serviceguard Manager
- **SNMP Access.** Allows setting the HP SIM central management server (CMS) as the trap target on selected HP-UX systems
- **System Management Homepage.** Displays the status of the management software and utilities installed on the system
- **System Page.** Displays all the information related to a specific system, including general information of the system, the status of the system, and a list of URLs that are related to the system
- **Version Control.** Uses HP Insight Management Agent (HP Version Control Repository Manager, HP Version Control Agent, and other agents) to facilitate Software Update and tasks related to it
- **HP ProLiant Essentials Virtual Machine Management Pack.** Enables you to deploy the HP ProLiant Essentials Virtual Machine Management Pack agent to target VM hosts
- **Webmin.** A Web-based interface for system administration for UNIX and is also used with Linux. Using HP SIM, you can setup user accounts, Apache, DNS, file sharing, and so on

Related Procedures

- New Command Line Tool
- New Copy a File Tool
- New Command Line Tool
- New Copy a File Tool
- Removing and Restoring Tools
- New Web Launch Tool
- New X Window Tool
- Setting Disk Thresholds
- Collecting Keys
- Deploying Keys
- Managing Keys
- Adding Keys From a File
- Adding Key Individually
- Viewing Key Database Contents
- Viewing Key Details
- Deleting Management Processor Users
- Deploying SSH Public Keys to Management Processors
- Editing Management Processor Users
- Upgrading Management Processor Firmware
- Executing Internal Control Actions through Management Processors
- Configuring LAN Access on Management Processors
- Configuring LDAP Settings on Management Processors
- Creating New Users on Management Processors
- Controlling the System Locator LED through Management Processors
- Controlling System Power Options through Management Processors

- [Compiling a MIB](#)
- [Editing a MIB](#)
- [Registering a MIB](#)
- [Unregistering a MIB](#)
- [Viewing a MIB](#)
- [Creating a New Custom Command](#)
- [Managing Custom Commands](#)
- [Property Pages](#)
- [Initial ProLiant Support Pack Install](#)
- [Deploying OpenSSH to Multiple Systems Using RDP](#)
- [Installing OpenSSH](#)
- [Creating a Replicate Agent Settings Task](#)
- [Discovering Storage Using SNMP](#)
- [Using HP Systems Insight Manager with SNMP Storage Solutions](#)
- [Installing RPM](#)
- [Querying RPM](#)
- [Uninstalling RPM](#)
- [Verifying RPM](#)
- [Accessing the System Management Homepage](#)
- [Editing System Properties for a Single System](#)
- [Suspending or Resuming System Monitoring for a Single System](#)
- [Installing Software and Firmware](#)
- [Accessing the Version Control Agent](#)
- [Accessing the Version Control Repository Manager](#)
- [Deploying the VMM Agent](#)

Related Topics

- [Command Line Tools](#)
- [Custom Commands](#)
- [Cluster Monitor](#)
- [Device Ping](#)
- [Disk Thresholds](#)
- [Configuring DMI Access](#)
- [Storage Integration Using SNMP](#)
- [License Manager](#)
- [Management Processor Tools](#)
- [Managing MIBs](#)
- [Partner Applications](#)
- [PMP Tools](#)
- [Process Resource Manager Overview](#)
- [Replicate Agent Settings - Reference](#)
- [RPM Package Manager](#)
- [HP Serviceguard Manager Overview](#)
- [Server Migration Pack](#)
- [Configuring SNMP Access](#)
- [System Management Homepage](#)
- [System Page](#)
- [Version Control](#)
- [Virtual Machine Management Pack](#)
- [Webmin Overview](#)

Cluster Monitor

Cluster Monitor enables you to monitor MSCS clusters.

To access the **Cluster Monitor** page, use of the following procedures:

1. Select **Tools->System Information->Cluster Monitor**.

Note: **Cluster Monitor** is not displayed in the menu if there are no MSCS clusters discovered.

2. Select a target MSCS cluster, and click **Run Now**. Refer to “Creating a Task” for more information on selecting a target cluster.

or

1. Locate a cluster by expanding **Systems** under the **Systems and Events** panel and selecting a cluster collection.

The appropriate cluster collection table appears in the workspace.

Note: Only the MSCS clusters you are authorized to access display on the cluster table view page.

2. Click the name of the MSCS cluster in the **Cluster Name** column.

or

Click the MSCS cluster status icon in the **CS** column on the cluster table view page.

The **Cluster Monitor** page appears for that cluster.

There are four tabs available on the **Cluster Monitor** page.

Note:



Every tab includes a **Problem Info** section that gives detailed information of any problems reported on the tab. For example, on the **Cluster** tab, this section includes status information if the cluster has a status of anything other than Normal.

Note:



Each tab also includes a **Last Update** field that displays the last time the information on the tab was updated.

- **Cluster.** Includes cluster information such as the cluster status, name, IP address, and quorum.
- **Nodes.** Includes node information such as the node status, name, and IP address.

- **Network.** Includes network information, such as the network status, name, mask, state, role, and description.
- **Resources.** Includes MSCS Resource information for the cluster including the status, name, IP address, state, group, owner node, type, and drive of the resources.

Related Topics

- Cluster Monitor Cluster Tab
- Cluster Monitor Nodes Tab
- Cluster Monitor Network Tab
- Cluster Monitor Resources Tab

Configuring Cluster Resource Settings

Configure the cluster-level resource settings to customize Cluster Resources for your environment.

Note:



When using the keyboard to input an alphanumeric character to highlight an option with the arrow keys in any dropdown list in the Cluster Monitor, press the **Enter** key to select the item.

To configure cluster resource settings:

1. Select **Options->Cluster Monitor->Cluster Resource Settings**. The **Cluster Monitor - Cluster Resource Settings** page appears.
2. Select **ALL (MSCS)** from the **Cluster Type** list to configure MSCS clusters.
3. Select **MSCS** from the **Resource** list.
4. Select **Polling** and set the polling rate.
Note: HP recommends setting the polling rate to no less than five minutes.
5. Click **OK** to save the changes.

Related Procedure

- Configuring Node Resource Settings

Related Topics

- Cluster Table View Page
- Cluster Monitor

Configuring Node Resource Settings

Configure the node-level resource settings to customize Cluster Monitor for your environment.

To configure node resource settings:

1. Select **Options->Cluster Monitor->Node Resource Settings**. The **Cluster Monitor - Node Resource Settings** page appears.
2. Select the cluster from the **Cluster** list at the top of the page. Select **All** to configure a resource the same for all clusters. To set polling values for CPU utilization or disk capacity, the cluster choice must be set to **All**.
3. Select the node from the **Node** list. Select **All** to configure a resource the same for all nodes in the selected cluster. As in the case of clusters in step 1, some resource attributes can only be set once for all nodes and so require you to select all clusters and nodes. Refer to the individual attribute descriptions for a particular resource.
4. Select the resource from the **Resource** list to display buttons for the resource configurable parameters.
5. Specify the appropriate resource options.

Note: HP recommends settings the polling rate to no less than five minutes.

Note: If you select **All** from the **Cluster** list and select **CPU** or **Disk** from the **Resource** list, you can set polling or threshold values. If you select **Polling**, set the value, then select **Thresholds**, set the values, and then select **Polling** again, the new polling values are still displayed. No matter when you click **OK** after setting the polling or thresholds values, these values are saved and not reset to the original value, which is the same when setting thresholds.

6. Click **OK** to save the changes.

Related Procedure

- Configuring Cluster Resource Settings

Related Topics

- Cluster Table View Page
- Cluster Monitor

Cluster Monitor Cluster Tab

The Cluster Monitor **Cluster** tab displays the following information for MSCS clusters:

- **Status.** Displays the cluster status. Cluster statuses include Critical, Major, Minor, Normal, and Unknown. Refer to "System Status Types" for more information on status types.
- **Name.** The cluster name or alias.
- **IP Address.** The IP address of the cluster alias.
- **Quorum.** Resource that maintains essential cluster data and guarantees that all nodes have access to the most recent database changes.

You can sort the information located on the **Cluster** tab by clicking a column heading. This sorts the information by that column in ascending or descending order.

The **Problem Info** section displays detailed information on any cluster status other than Normal.

Related Topics

- Cluster Monitor
- Cluster Monitor Nodes Tab
- Cluster Monitor Network Tab
- Cluster Monitor Resources Tab
- System Status Types

Cluster Monitor Nodes Tab

The Cluster Monitor **Node** tab displays the following information for MSCS clusters:

- **Status.** Displays the node status. Node statuses include Critical, Major, Minor, Normal, Failed, and Unknown. Refer to “System Status Types” for more information on node status types.
- **Name.** The node name.
- **IP Address.** The IP address of the node.

You can sort the information located on the **Nodes** tab by clicking a column heading. This sorts the information by that column in ascending or descending order.

The **Problem Info** section displays detailed information on any node status other than Normal.

Related Topics

- Cluster Monitor
- Cluster Monitor Cluster Tab
- Cluster Monitor Network Tab
- Cluster Monitor Resources Tab
- System Status Types

Cluster Monitor Network Tab

The Cluster Monitor **Network** tab displays the following information for MSCS clusters:

- **Status.** Displays the network status. Network statuses include Critical, Major, Minor, Normal, Disabled, and Unknown. Refer to “System Status Types” for more information on network status types.
- **Name.** Server cluster object that carries internal communication between nodes and provides client access to cluster resources.
- **Mask.** The subnet mask associated with the network within the cluster.
- **State.** The state of the network: Normal (the network state is online or available), Degraded (the network is partitioned), Failed (the network state is offline), and Other (the network state indicates that an error has occurred and the exact state of the network could not be determined or the network state is unavailable).
- **Role.** Role the network name plays in the cluster: network name for the cluster, network name for computer systems in the cluster, or network name for groups in the cluster.

- **Description.** Description of the network

You can sort the information located on the **Network** tab by clicking a column heading. This sorts the information by that column in ascending or descending order.

The **Problem Info** section displays detailed information on any network status other than Normal.

Related Topics

- Cluster Monitor
- Cluster Monitor Cluster Tab
- Cluster Monitor Nodes Tab
- Cluster Monitor Resources Tab
- System Status Types

Cluster Monitor Resources Tab

The Cluster Monitor **Resources** tab displays the following information for MSCS clusters:

- **Status.** Displays the resource status. Resource statuses include Critical, Major, Monitor, Normal, and Unknown. Refer to "System Status Types" for more information on network status types.
- **Name.** Physical or logical entity that is capable of being owned by a node, brought online and taken offline, moved between nodes, and managed as a server cluster object.
- **IP.** The IP address of the cluster.
- **State.** State of the resource: Normal (the resource state is online), Degraded (the resource state is Unavailable, Offline, Online, Pending, or Offline Pending), Failed (the resource state is failed), and Other (unable to determine the resource condition).
- **Group.** Collection of resources managed as a single server cluster object.

Note: A group must have a network name and an IP address associated with it for you to access group resources. A group can be owned by any node in the cluster and can be moved by users with full-configuration-rights for load balancing and other administrative purposes. When a failure takes place, the entire group fails over, that prompts the cluster software to transfer all group resources and data to a different node in the cluster. The resources and data in a transferred (failed over) group are still accessible under the same network name and IP address, even after they have been moved to a different node.

- **OwnerNode.** Node on which a resource resides.
- **Type.** Server cluster object used to categorize and manage resources that have similar characteristics.
- **Drive.** Disk or drive on which the resource resides.

The **Last update** field displays the date and time of the last update of the information included on the tab. The **Problem Info** section includes detailed information on any resource problems reported.

The **Problem Info** section displays detailed information on any resource status other than Normal.

Related Topics

- Cluster Monitor
- Cluster Monitor Cluster Tab
- Cluster Monitor Nodes Tab
- Cluster Monitor Resources Tab
- System Status Types

MSCS Status

Monitoring MSCS Status

HP Systems Insight Manager (HP SIM) monitors Microsoft Clustering Service (MSCS) status on each monitored Windows cluster and displays it as a cluster attribute in the Cluster Monitor. It is a contributor to the cluster status shown in the **CS** column on the cluster table view page. Cluster Monitor polls the cluster on a set interval to retrieve the status value.

Refer to “Cluster Monitor Polling Rate” for information on MSCS Resource Settings.

To access the **Cluster Monitor - Cluster Resource Settings** page, click (**Options->Cluster Monitor->Cluster Resource Settings**).

Note:



Only users with full-configuration-rights can change the polling values.

Related Topics

- Cluster Monitor
- Cluster Resources Supported by HP Systems Insight Manager

Cluster Resources Supported by HP Systems Insight Manager

HP Systems Insight Manager (HP SIM) supports several Cluster Monitor resources:

- Disk
- CPU
- System

The System resource monitors the system health of the cluster member.

Disk and CPU resources monitor the Disk capacity and CPU utilization, respectively. You can set minor and major thresholds for individual nodes in a cluster. When those thresholds are reached, Cluster Monitor creates an HP SIM event. The event triggers associated e-mail and paging notification as configured in the HP SIM options.

Cluster Monitor States

Note:



The cluster condition is Other when all the nodes of a cluster are down.

The following table explains the condition categories for each list.

List	Normal	Degraded	Failed	Other
Node	The node status is an active cluster member.	The node status is down, trying to reform or rejoin a cluster, is operating as an active member of a cluster but cannot host any resources or resource groups, or is up but cluster activity is paused.	The node status is down or trying to form or rejoin a cluster.	The node status is Unavailable or could not be determined.
Network	The network state is Online or Available.	The network state is Partitioned.	The network state is Offline.	The network state indicates that an error has occurred and the exact state of the network could not be determined or the network state is unavailable.
Resources	The resource state is Online.	The resource state is Unavailable, Offline, Online Pending, or Offline Pending.	The resource state is Failed.	The resource state is Unknown.

Note:



For additional information about the Microsoft Cluster Service, refer to Microsoft's documentation.

Related Topic

- Cluster Monitor

Cluster Monitor Resources and Associated Settings

Note:



Although Cluster Monitor is used for MSCS clusters only, the CPU and Disk thresholding functionality for Cluster Monitor works for any cluster in which the cluster nodes are running HP Insight Management Agents.

This version of HP Systems Insight Manager (HP SIM) includes these node-level cluster monitor resources and associated settings:

- CPU (refer to “Cluster Monitor Polling Rate” or “Cluster Monitor Resource Thresholds”)
 - Disk (refer to “Cluster Monitor Polling Rate” or “Cluster Monitor Resource Thresholds” for clusters)
 - System (refer to “Cluster Monitor Polling Rate” for nodes)
-

Note:



Refer to “Cluster Resources Supported by HP Systems Insight Manager” for information about the CPU utilization data.

Related Procedures

- Customizing System or Cluster Collections
- Performing an Advanced Search for Clusters

Related Topics

- Cluster Monitor
- Searching for Systems and Events
- Cluster Resources Supported by HP Systems Insight Manager
- Cluster Table View Page
- Navigating the Systems and Events Panel

Cluster Monitor Polling Rate

Polling Rates

Note:



You can specify only one polling rate (interval) for all nodes in all clusters. You cannot specify different rates for different nodes, so the polling fields display on the

configuration page only when you select **All** in both the **Cluster** and **Node** dropdown lists.

CPU Polling Rate

The CPU polling rate determines how often Cluster Monitor checks CPU utilization as reported by the appropriate HP Insight Management Agent on monitored nodes.

Adjust the CPU polling rate by configuring the Cluster Monitor's node resource settings. Refer to "Configuring Node Resource Settings" for more information on configuring the node resource settings.

Disk Polling Rate

The Disk polling rate determines how often Cluster Monitor checks the free disk space as reported by the appropriate HP Insight Management Agent on monitored nodes.

Adjust the polling rate by configuring the Cluster Monitor's node resource settings. Refer to "Configuring Node Resource Settings" for more information on configuring the node resource settings.

MSCS Status Polling Rate

The polling rate you enter determines how often Cluster Monitor checks the MSCS status of monitored clusters.

Adjust the status polling rate by configuring the Cluster Monitor's cluster resource settings. Refer to "Configuring Cluster Resource Settings" for more information on configuring the cluster resource settings.

System Status Polling Rate

The system polling rate determines how often Cluster Monitor checks node status as reported by the appropriate HP Insight Management Agent running on the nodes.

System is a node-level attribute, so adjust the polling rate by configuring Cluster Monitor's node resource settings. The polling rate is a global attribute of the resource, so you can specify only one polling interval for all nodes in all clusters. The polling fields display on the configuration page only when you select **All** in both the **Cluster** and **Node** dropdown lists.

Related Procedures

- Configuring Cluster Resource Settings
- Configuring Node Resource Settings

Related Topic

- Cluster Monitor

Cluster Monitor Resource Thresholds

Threshold Overview

Cluster resources use thresholds to trigger HP Systems Insight Manager (HP SIM) events. The Disk resource sets thresholds for disk capacity, and the CPU resource sets thresholds for CPU utilization.

Disk Capacity Thresholds

The Disk resource collects disk capacity data. To access the **Cluster Monitor - Node Resource Settings** page where the thresholds are set, select **Options->Cluster Monitor->Node Resource Settings**.

The threshold values you enter in the **Settings for the Selected Resource** section define the Normal, Minor, and Major ranges for disk utilization on monitored nodes.

For each disk, there are four thresholds in pairs. The Minor and Major thresholds are each associated with a corresponding reset threshold. Utilization enters the Major range when it equals or exceeds the Major threshold value and remains in the Major range until it falls to or below the Major reset value. The Minor and Major reset thresholds behave similarly.

You can specify different thresholds for each disk in each node of a cluster.

Refer to “Configuring Node Resource Settings” for more information on setting disk thresholds.

CPU Utilization Thresholds

The CPU resource collects utilization data for the CPUs in a particular. To access the **Cluster Monitor - Node Resource Settings** page where the thresholds are set, select **Options->Cluster Monitor->Node Resource Settings**.

The threshold values you enter in the **Settings for the Selected Resource** section define the Normal, Minor, and Major ranges for CPU utilization on the selected node.

For each CPU, there are four thresholds in pairs. The Minor and Major thresholds are each associated with a corresponding reset threshold. Utilization enters the Major range when it equals or exceeds the Major threshold value and remains in the Major range until it falls to or below the Major reset value. The Minor and Major reset thresholds behave similarly.

You can specify different thresholds for each CPU in each node of a cluster.

Refer to “Configuring Cluster Resource Settings” for more information on CPU thresholds.

Related Topic

- Cluster Monitor

Command Line Tools

Use the command line interface (CLI) tools to execute basic UNIX and Windows commands remotely on one or more systems.

Note:



For additional information about the individual commands, refer to the associated manpage on an HP-UX and Linux system or the Windows command line help where the command tool is installed.

Note:



Command line tools provided by HP-UX and Linux, such as **ls** and **df**, are run as root by default. For security reasons, you might want them to run as a specific user to avoid permitting unintended capabilities to a user.

To launch a command line tool:

1. Select **Tools->Command Line Tools->UNIX/Linux** for Linux or UNIX command line tools.
or
Select **Tools->Command Line Tools->Windows** for Windows command line tools.
2. Select the command line tool that you want to run, and follow the steps to launch the tool. Refer to “Creating a Task” for assistance with the steps.
3. Click **Run Now** to launch the tool.

Command Line Interface

Use the **mxexec** command to launch these command tools on one or more systems from the command line interface. For assistance with this command, refer to the associated manpage. Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Topics

- Using Command Line Interface Commands
- Managing with Tasks
- Viewing Task Results

Creating New Command Line Tools

Note:



These tools are only available on HP-UX and Linux central management server CMS systems, not on a Windows CMS.

The New Command Line tools are part of a distributed task facility (DTF) and one of the tools available in HP Systems Insight Manager (HP SIM) to run on single-system aware (SSA) systems. Users with full-configuration-rights can create a new command line tool. The created tool appears under the **Command Line Tools** menu, and then you can schedule when the tool runs.

The new tools available are:

- **New Command Line Tool.** Select **Tools->Command Line Tools->New Command Line Tools->New Command Line Tool**. The **New Command Line Tool** page appears.
- **New Copy a File Tool.** Used to create a tool that copies a script and executes if desired. Select **Tools->Command Line Tools->New Command Line Tools->New Copy a File Tool**. The **New Copy a File Tool** page appears.
- **New X Window Tool.** Select **Tools->Command Line Tools->New Command Line Tools->New X Window Tool**. The **New X Window Tool** page appears.

Related Procedures

- New Command Line Tool
- New Copy a File Tool
- Removing and Restoring Tools
- New Web Launch Tool
- New X Window Tool

Related Topic

- Command Line Tools Reference
- Examples of Using Parameter Strings in Command Line Tools

New Command Line Tool

Use this tool to create a simple command line tool that runs on target single-system aware (SSA) systems. This tool creates a temporary XML tool definition file under `/var/tmp` then loads it with the command `mxtool -af file`. You only need to enter data into the required fields.

Warning!



If you define this tool to run as root, any user authorized to run this tool might be able to gain full access to the managed system depending on how you define the command and what its capabilities are. Otherwise, the tool runs as the HP Systems Insight Manager (HP SIM) user and that user's SSH public key must be configured on the managed system using the `mxagentconfig` command.

To create a new command line tool:

1. Select **Tools->Command Line Tools->New Command Line Tools->New Command Line Tool**. The **New Command Line Tool** page appears.
2. Under **Parameters**, add information using the standard tool parameters. The following fields are required:

- Tool name
 - Tool command (with parameter if needed)
3. Click **Run Now** to run the task to create a new tool immediately or click **Schedule** to schedule when the task runs. Refer to “Scheduling a Task” for more information on scheduling a task.

Additional Information

Additional information is available in the following sections:

- “Tool Types”
- “Parameterized Strings”
- Command Line Tools - Parameterized Strings Substitution Table [useTools_commandLineTools_ref.html#SubstitutionTable]
- “Tool Filtering”
- “Version Numbers”
- “Other Requirements”
- “Document Type Definition”

Related Procedures

- New Copy a File Tool
- Removing and Restoring Tools
- New Web Launch Tool
- New X Window Tool

Related Topics

- Command Line Tools
- Command Line Tools Reference
- Examples of Using Parameter Strings in Command Line Tools

New Copy a File Tool

This tool creates a command line tool that copies a file to each single-system aware (SSA) system then runs a command (which could be that file if it is a script). Note that the source and target paths of the file to copy must to be different.

This tool creates a temporary XML tool definition file under `/var/tmp`, then loads it with the command `mxttool -af file`. You only need to enter data into the required fields.

Warning!



If you define this tool to run as root, any user authorized to run this tool might be able to gain full access to the managed system, depending on how you define the command and what its capabilities are. Otherwise, the tool runs as the HP Systems Insight Manager (HP SIM) user and that user's SSH public key must be configured on the managed system using the **mxagentconfig** command.

To create a new copy file tool:

1. Select **Tools->Command Line Tools->New Command Line Tools->New Copy a File Tool**. The **New Copy a File Tool** page appears.
2. Under **Parameters**, add information using the standard tool parameters. The following fields are required:
 - Enter tool name
 - Enter source path on central management server
 - Enter target path on managed system
 - Enter command

Refer to Example of Creating a Copy a File Tool for an example of filling in the parameters.

3. Click **Run Now** to run the task immediately or click **Schedule** to schedule when the task runs. Refer to "Scheduling a Task" for more information on scheduling a task.

Additional Information

Additional information is available in the following sections:

- "Tool Types"
- "Parameterized Strings"
- Command Line Tools - Parameterized Strings Substitution Table
[useTools_commandLineTools_ref.html#SubstitutionTable]
- "Tool Filtering"
- "Version Numbers"
- "Other Requirements"
- "Document Type Definition"

Example of Creating a Copy a File Tool

The following is a simple example to copy a script file (name `myScript`) to a target system then execute the script.

1. In the **Enter tool name** field, enter a name for the new tool, such as **My Script**.

2. In the **Enter source path on central management server** field. For example, `/home/user name/myScript`.
3. In the **Enter target path on managed system**, enter the path where you want to save the tool. For example, `/tmp/myScript`.
4. In the **Enter command** field, enter the command to execute the tool on the managed system. For example, `sh/rmp/myScript`.

Related Procedures

- New Command Line Tool
- Removing and Restoring Tools
- New Web Launch Tool
- New X Window Tool

Related Topics

- Command Line Tools
- Command Line Tools Reference
- Examples of Using Parameter Strings in Command Line Tools

New X Window Tool

Use this tool to create an X Window command line tool that runs on a target system. This tool creates a temporary XML tool definition file under `/var/tmp` then loads it with the command `mxtool -af file`. You only need to enter data into the required fields.

Warning!



If you define this tool to run as root, any user authorized to run this tool might be able to gain full access to the managed system depending on how you define the command and what its capabilities are. Otherwise, the tool runs as the HP Systems Insight Manager (HP SIM) user and that user's SSH public key must be configured on the managed system using the `mxagentconfig` command.

1. Select **Tools->Command Line Tools->New Command Line Tools->New X Window Tool**. The **New X Window Tool** page appears.
2. Under **Parameters**, add information using the standard tool parameters. The following fields are required:
 - Tool name
 - Tool command (with parameter if needed)
3. Click **Run Now** to run the task immediately or **Schedule** to schedule when the task runs. Refer to "Scheduling a Task" for more information on scheduling a task.

Additional Information

Additional information is available in the following sections:

- “Tool Types”
- Command Line Tools - Parameterized Strings Substitution Table [useTools_commandLineTools_ref.html#SubstitutionTable]
- “Tool Filtering”
- “Version Numbers”
- “Other Requirements”
- “Document Type Definition”

Related Procedures

- New Command Line Tool
- Removing and Restoring Tools
- New Web Launch Tool
- New Copy a File Tool

Related Topics

- Command Line Tools
- Command Line Tools Reference
- Examples of Using Parameter Strings in Command Line Tools

Command Line Tools Reference

Tool Types

There are five basic types of HP Systems Insight Manager (HP SIM) tools, single-system aware (SSA) tools, multiple-system aware (MSA) tools, and Web-launch aware (WLA) tools.

SSA tools are executed on a target system and are only aware of the target system environment. When executing an SSA tool, therefore, the distributed task facility (DTF) sends the tool information to each HP SIM agent to execute the tool. An example of an SSA tool would be a tool that wraps a common UNIX command, such as **ls**, **cat**, or **cp**.

MSA tools are executed on a central system, sometimes the central management server (CMS), and know how to handle a list of target systems. An example of an MSA tool would be a tool that wraps the functionality of Ignite-UX on HP-UX systems.

WLA tools are tools that are generally executed in a browser and are specified by a universal resource location (URL).

Parameterized Strings

To create tools properly, the tool developer must understand how URLs and command lines are formed. Using parameterized strings, tool developers can greatly enhance the options available in creating tool definition files (TDEFs).

Parameterized strings are strings which contain replacement fields, similar to the format strings used in the popular printf() function in the standard C library. These fields can be replaced by values entered by the user at runtime (as defined by the tool parameters attribute), by some standard task properties supplied by the Task Controller, values related to the selected target systems or system groups, or by property values retrieved from a global tool properties file. This allows a very specific URL or command line to be generated.

Parameterized Strings Substitution Table

The following parameters provide substitution of global attribute values:

Parameter	Description
%t	Task ID for the task being executed
%u	Name of the user running this tool
%e	Name of the user to execute this tool as
%s	Management server hostname of the core CMS running the tool
%#	(where # is a positive integer) Substitute the value input by the user for the parameter referenced by the number (#) provided, as a list index position (one-based... %1, %2, %3, and so on)
%y	SOAP logon token, for use with SOAP single sign-on Web applications

The following parameters provide substitution of the current selected target:

Parameter	Description
%f	The database name of the target system (or system group, if the %x toggle was in the string).
%n	Network name (hostname, IP address, IPX address, or system name in that order).
%a	Network address (IP address, or IPX address, in that order).
%l	Link name in format specified by System Link Configuration setting (name, IP address, or full DNS name).
%p	IP address of WBEM proxy, if any, for this target, in the form <ip address>:<port#></port#></ip>.
%g	Database GUID of the target system (or system group, if the %x toggle was in the string).
%b	System type of the target system.
%c	System sub-type of the target system

Parameter	Description
<code>%r% (rt[.attribute]%)</code>	Substitutes the related system that has the relationship type as specified in the parameter "rt." If the [.attribute] is specified, then one of the named system attributes would be returned for the related system. In addition, the common attributes such as Network name (.a) also work. For example, to get the server's management processor's IP address, use <code>%r{MgmtProcToServer.a%}</code> to get the contact use <code>%r{MgmtProcToServer.Contact%}</code> . If the related systems attribute is omitted then for each system, the network name and IP address is returned. The network name and IP address is returned in the form "network name ip address" if more than one system is returned, then they are comma-delimited. Note that the relationship type "MgmtProcToServer" can be used to return related system information for all management processor relationship types.
<code>%(attribute)%</code>	The value of the named attribute of the target system.

The following parameters provide repetition to support multiple selected target systems:

Parameter	Description
<code>%(... %)</code>	Repeated pattern (only repeats if a current selection exists). If a current target selection does not exist, the text between the delimiters is removed on expansion. This allows the text to be optional and dependent upon the target selection list.
<code>%i</code>	Selection index (one-based).
<code>%z</code>	Do not substitute anything, but increment the selection index to the next integer and the referenced target system to the next target in the selected target list.
<code>% <... > </code>	Encrypted text (encrypt after all other parameters have been substituted).
<code>%%</code>	Enables you to retain a % in the command/URL after substitution.

Tool Filtering

Tool filtering is a facility enabling the tool writer to control whether the tool should be executed on a selected system. Most tools are platform dependent in that their successful execution depends on commands that are provided on some platforms but not on others. For example, the `bdF` tool depends on the `bdF` command, which is provided on HP-UX platforms, but is not available under that name on Linux platforms. A tool should only be visible in the **Tools** menu when there is at least one discovered system that passes the filter requirements. A discovered system must pass the

filter requirements and is then executed only if all the filter requirements are passed. To do this, the tool specifies in a system filter expression the system attributes that must be possessed by all systems it can run on.

The system attributes required for a tool to run are specified by system filter expressions having the form:

```
<system-filter name="attribute-name" operator="eq"
  value="attribute-value" />
  or
<system-filter name="attribute-name" operator="ge"
  value="attribute-value" />
  or
<system-filter name="attribute-name" operator="lt"
  value="attribute-value" />
  or
<system-filter name="attribute-name" operator="ct"
  value="attribute-value" />
  or
<system-filter name="attribute-name" operator="neq"
  value="attribute-value" />
  or
<system-filter name="attribute-name" operator="nct"
  value="attribute-value" />
```

The eq operator the system on which the tool can run must have exactly the attribute value specified. It applies to any attribute name allowed in a system filter expression. The ge operator specifies that a system on which the tool can run on must have at least the attribute value specified. The lt and ge operators can only be used with revision attributes, specifically OSRevision in the OS type filter and all of the attributes of the Protocol type filter. The value of these attributes can be numeric or can be character strings. The ct operator specifies that a system on which the tool can run on must have an attribute that contains the value specified. The neq operator specifies that a system on which the tool can run on must not have the exact attribute value specified. It applies to any attribute name allowed in a system filter expression. The nct operator specifies that a system on which the tool can run on must have the attribute that does not contain the value specified. For systems, the numeric valued attributes the filter expression can specify include the *OSRevision* and *Protocol Support* attributes, whose values are version numbers. The values permitted for version numbers and how they are compared is described in the Version Numbers in the following section. The attribute-name is one of the values listed in the tables in the following section, or a protocol name from the ProtocolSupport attribute of a system. The attribute-value is one of the possible system attribute values for attribute-name.

Attribute values are based on the Distributed Task Force (DMTF) Common Information Model (CIM). Usually these values are defined during the system identification process, which uses WBEM and SNMP to determine system attributes. For this release, valid OSName values are HP-UX and Linux. For an OSName value of HP-UX, the OSRevision attribute values have the leading alphabetic field removed (for example B.11.11 is stored as 11.11).

A system filter expression is used as part of an include filter expression. There are three types of include filter expressions, each allowing a different category of attribute names on which to be filtered.

Category	Filter Type	Attribute Names Allowed
Operating System	os	OSName, OSVendor, OSRevision
Hardware	hardware	DeviceType, DeviceSubType, Model
Protocol Support	protocol	Any protocol name, except HTTP
Other	other	Can be any predefined system attribute or any custom-system attribute.

An include filter includes one or more system filter expressions using the attributes names allowed for it. For example, an os filter could consist of:

```
<include-filter type="os">
  <system-filter name="OSName"
operator="eq" value="LINUX" />
  <system-filter name="OSVendor"
operator="eq" value="RedHat" />
  <system-filter name="OSRevision"
operator="ge" value="7.2" />
</include-filter>
```

The include filter need not include all attributes allowed. If more than one attribute is included, the conditions are logically and'ed together. An attribute cannot appear in an include filter more than once, except that an attribute having a version number value can appear twice if one operator is lt and the other operator is ge. For example:

```
<include-filter type="protocol">
  <system-filter name="WBEM"
operator="lt" value="2.6" />
  <system-filter name="WBEM"
operator="ge" value="2.4" />
</include-filter>
```

This would specify that the tool should be shown for any collection of systems supporting the WBEM protocol version 2.4 or higher, but less than 2.6.

If a tool contains more than one include filter of different types, the conditions of the filters are logically AND'd together. A tool with both Operating System and Hardware dependencies could use the filter:

```
<include-filter type="os">
  <system-filter name="OSName"
    operator="eq" value="LINUX" />
</include-filter>
<include-filter type="hardware">
  <system-filter name="DeviceSubType"
    operator="eq" value="HPVectra" />
</include-filter>
```

If a tool contains more than one include filter of the same type, the conditions of the filters are logically or'ed together. A tool available on two different operating systems could specify:

```
<include-filter type="os">
  <system-filter name="OSName"
    operator="eq" value="LINUX" />
</include-filter>
<include-filter type="os">
  <system-filter name="OSName"
    operator="eq" value="HPUX" />
</include-filter>
```

This tool could be launched on any collection of systems using Linux or HP-UX.

Tool filtering depends on the attributes being filtered having a value defined on the systems selected. For the "os" filter type, if any attributes being filtered on are not defined for a system, the system is assumed to have the value required by the filter. Thus a system with none of the os attributes specified by a tool filter will be assumed capable of running the tool. For the hardware filter type, the above statement is true in the case of the Model attribute. But for the DeviceType and DeviceSubType attributes, the tool filter will apply only for known values on the selected systems. The *protocol* filter type requires that the protocol must exist on the system before the operators can be applied. This means that the neq and nct operators also depend on the system to have that protocol. The other filter also works like the protocol filter such that the attribute being filtered upon must exist on the system before the operators can be applied. If a tool uses the other and/or protocol filters, then at least one system must contain the filterable attributes for the tool to be displayed in the GUI.

Version Numbers

The OSRevision and Protocol Support system attributes have values that are interpreted as version numbers if possible. A version number is a series of non-negative decimal numbers separated by period (.) characters. When comparing version numbers, the following rules are used:

- The leftmost numbers in the series are most significant, so 1.0 is greater than 0.1.
- Leading zeroes on the numbers are disregarded, so 003 is equal to 3.
- Two adjacent period characters are interpreted as if they delimited the number zero, so 1.0.3 is equal to 1..3
- A beginning period character is interpreted as if preceded by a zero, so .9 is equal to 0.9.
- Trailing zero numbers are disregarded, so 1.0.0 is equal to 1.

Other Requirements

SSA command tools must contain an execute statement (`execStmt`) or a file copy statement (`copyStmt`), or both. If only the execute statement is specified, no files are copied prior to executing the command. If only a file copy statement is specified, after the file(s) are copied, no command is executed. If they are both specified, the files are copied first and then the command is executed.

MSA command tools must specify a command and the system on which the command will execute.

Tool names must be at least one character in length, and no more than 256 characters in length. The first character of the name must be alphabetic. Characters after the first can be letters, digits, spaces, or any of the characters - . () or _.

Web launch aware tools must specify a main URL.

When specifying file copy pairs, the destination file paths for each file copy pair within a single tool definition must be unique. Specifying the same destination file path for multiple source file paths results in a file parsing error.

An error occurs when running a tool that copies a file if the file does not exist or is unreadable. The source file path is not checked at the time the tool is created or modified, but must exist at the time the tool is executed.

When the log element is set to true, standard out and standard error output from the execution of the tool is logged in the central management server (CMS) log file `/var/opt/mx/logs/mx.log`. When it is set to false, only summary task log information, such as start and end times and task status is logged.

Document Type Definition

The Document Type Definition (DTD) file defines the constraints for an XML file. These constraints include the valid element tags, attributes, and the cardinality of elements in an XML file. The tool DTD file is named `toollist.dtd` and is included in the following paragraph. Note that due to manpage formatting, the DTD contents might not appear the same as in the file.

```
<?xml version="1.0" encoding="UTF-8" ?>

<!-- The tool-list element can contain zero or more of
      ssa-command-tool elements, msa-command-tool elements,
      web-launch-tool elements, automation-tool elements or
      app-launch-tool elements.-->

<!ELEMENT tool-list ( ssa-command-tool |
                      msa-command-tool |
                      web-launch-tool |
                      automation-tool |
                      app-launch-tool )* >

<!-- The ssa-command-tool element specifies a single-system aware
      tool. The ssa-command-tool element can optionally specify a
      category element, a description element, a comment element, an
      owner element, a default-target element, an execute-as-user
      element, a job-display-handler element, a toolbox-enabled
      element, zero or more toolbox elements, zero or more
      include-filter elements, or zero or more env-variable elements.
      (NOTE: The role-enabled and role elements are deprecated
      elements and should not be used with this product. These
      are provided for backward compatibility with previous
      products. The toolbox-enabled element and the toolbox
      element should be used in their stead.)
      If more than one of these elements are specified, the element
      must appear in the order as listed in this definition. The
      ssa-command-tool element must contain an ssa-block element. The
      ssa-block element must appear after the previously described
      optional elements, if any of the optional elements are
      specified. Following the ssa-block element, one can specify zero
      or more attribute elements.-->

<!ELEMENT ssa-command-tool (category?, description?, comment?,
                            owner?, default-target?, execute-as-user?,
                            job-display-handler?,
                            toolbox-enabled?, toolbox*,
                            role-enabled?, role*,
                            include-filter*, env-variable*,
                            ssa-block, attribute* ) >

<!-- In addition to the previously described elements, the
      ssa-command-tool element specifies the following attributes. The
      name attribute specifies the tool name and must be specified in
      the ssa-command-tool element. The visible attribute specifies
      whether the tool is visible for running. By default tools are
      visible. The max-targets attribute specifies the maximum number
      of targets against which a tool can run. The revision attribute
      allows a tool author to specify a revision for the tool. Note
      that this is for information only. The job-log attribute
      specifies whether the results of the command will be kept in this
      system's job log. This attribute applies only to tools when they
      are run as scheduled tasks, not when they are run as "run now"
      tasks. When job-log="true" the job and target status for the tool
```

will be kept for a relatively lengthy system-defined period in the database after the job completes. When `job-log="false"` only the last completed copy of the job and target status for the task will be kept in the cache for a much shorter period of time, and will not be written to the database. Job logging is enabled by default. The `schedulable` attribute specifies whether the tool can be run as a schedulable task. When `scheduled="false"` the tool can only run as a "run now" task. Tools are scheduled by default. The `GUID` attribute specifies a globally unique identifier (GUID) for the tool. Because the system generates a GUID for a tool during the add operation, this field should only be specified during a modify operation. The `accepts-targets` attribute specifies whether the tool accepts targets for execution. The `accepts-targets` attribute is true by default. -->

```
<!ATTLIST ssa-command-tool name          CDATA    #REQUIRED
    visible      (true | false) "true"
    max-targets  NMTOKEN #IMPLIED
    revision     CDATA    #IMPLIED
    job-log      (true | false) "true"
    schedulable (true | false) "true"
    guid        NMTOKEN #IMPLIED
    accepts-targets (true|false) "true" >
```

```
<!-- The ssa-block specifies the elements specific to a single-system
aware tool. The ssa-block can specify a command or copy-block or
both. Only one command should be specified but up to 16 multiple
copy-blocks can be specified. After the command and/or
copy-blocks, one can specify the parameters for the command
and/or copy-block. -->
```

```
<!ELEMENT ssa-block (( command | copy-block )+, parameter*) >
```

```
<!-- The copy-block specifies a source file path and a destination
file path for a copy operation. -->
```

```
<!ELEMENT copy-block ( source, destination )+ >
```

```
<!-- The source element specifies the source file path for a copy
operation. -->
```

```
<!ELEMENT source (#PCDATA) >
```

```
<!-- The destination element specifies the destination file path for a
copy operation. -->
```

```
<!ELEMENT destination (#PCDATA) >
```

```
<!-- The msa-command-tool element specifies a multiple-system aware
tool. The msa-command-tool element can optionally specify a
category element, a description element, a comment element, an
owner element, a default-target element, an execute-as-user
element, a job-display-handler element, a toolbox-enabled
element, zero or more toolbox elements, zero or more
```

include-filter elements, or zero or more env-variable elements. (NOTE: The role-enabled and role elements are deprecated elements and should not be used with this product. These are provided for backward compatibility with previous products. The toolbox-enabled element and the toolbox element should be used in their stead.)

If more than one of these elements are specified, the element must appear in the order as listed in this definition. The msa-command-tool element must contain an msa-block element. The msa-block element must appear after the previously described optional elements, if any of the optional elements are specified. Following the msa-block element, one can specify zero or more attribute elements.-->

```
<!ELEMENT msa-command-tool (category?, description?, comment?, owner?,
    default-target?, execute-as-user?,
    job-display-handler?,
    toolbox-enabled?, toolbox*,
    role-enabled?, role*,
    include-filter*, env-variable*,
    msa-block, attribute* ) >
```

```
<!-- In addition to the previously described elements, the
    msa-command-tool element specifies the following attributes. The
    name attribute specifies the tool name and must be specified in
    the msa-command-tool element. The visible attribute specifies
    whether the tool is visible for running. By default tools are
    visible. The max-targets attribute specifies the maximum number
    of targets against which a tool can run. The revision attribute
    allows a tool author to specify a revision for the tool. Note
    that this is for information only. The job-log attribute
    specifies whether the results of the command will be kept in this
    systems job log. When job-log="true" the job and target status
    for the tool will be kept for a relatively lengthy system-defined
    period in the database after the job completes. When
    job-log="false" only the last completed copy of the job and
    target status for the tool will be kept in the cache for a much
    shorter period of time, and will not be written to the database.
    Job logging is enabled by default. The schedulable attribute
    specifies whether the tool can be run as a scheduled task. When
    schedulable="false" the tool can only run as a "run now" task.
    Tools are schedulable by default. The guid attribute specifies a
    globally unique identifier (GUID) for the tool. Because the
    system generates a GUID for a tool during the add operation, this
    field should only be specified during a modify operation. The
    accepts-targets attribute specifies whether the tool
    accepts targets for execution. The accepts-targets attribute is
    true by default. -->
```

```
<!ATTLIST msa-command-tool name          CDATA    #REQUIRED
    visible      (true | false) "true"
    max-targets  NMTOKEN #IMPLIED
    revision     CDATA    #IMPLIED
    job-log      (true | false) "true"
```

```
    schedulable (true | false) "true"
    guid        NMTOKEN #IMPLIED
    accepts-targets (true|false) "true" >

<!-- The msa-block specifies the elements specific to a
multiple-system aware (MSA) tool. The msa-block can specify an
MSA command, the parameters for the command and an execution system
on which the command executes. -->

<!ELEMENT msa-block ( command, parameter*, execution-system ) >

<!-- The command element specifies the command for an SSA or an MSA
tool. If the command accepts parameters, it must be specified as
a parameterized string. -->

<!ELEMENT command ( #PCDATA ) >

<!-- The command element can have two attributes. The command-type
attribute specifies whether the command is an x-window, stdout,
restart, launch, or an unknown command type. The default command
type is stdout. The log attribute specifies whether the results
of the command will be output to this system's audit log. When
log="true" the stdout and stderr results of the command will be
output to the system's audit log. Command output is not logged
by default. -->

<!ATTLIST command command-type (x-window |
stdout      |
restart    |
launch     |
unknown) "stdout"
log (true | false) "false" >

<!-- The execution-system element specifies the system on which an MSA
tool will execute. -->

<!ELEMENT execution-system ( #PCDATA ) >

<!-- The web-launch-tool element specifies a web launch tool. The
web-launch-tool element can optionally specify a category
element, a description element, a comment element, an owner
element, a default-target element, an execute-as-user element, a
job-display-handler element, a toolbox-enabled element, zero or
more toolbox elements, zero or more include-filter elements, or
zero or more env-variable elements.
(NOTE: The role-enabled and role elements are deprecated
elements and should not be used with this product. These
are provided for backward compatibility with previous
products. The toolbox-enabled element and the toolbox
element should be used in their stead.)
If more than one of these elements are specified, the element
must appear in the order as listed in this definition. The
web-launch-tool element must contain a web-block element. The
web-block element must appear after the previously described
```

optional elements, if any of the optional elements are specified. Following the web-block element, one can specify zero or more attribute elements.-->

```
<!ELEMENT web-launch-tool (category?, description?, comment?, owner?,
    default-target?, execute-as-user?,
    job-display-handler?,
    toolbox-enabled?, toolbox*,
    role-enabled?, role*,
    include-filter*, web-block, attribute* ) >
```

```
<!-- In addition to the previously described elements, the
    web-launch-tool element specifies the following attributes. The
    name attribute specifies the tool name and must be specified in
    the web-launch-tool element. The visible attribute specifies
    whether the tool is visible for running. By default tools are
    visible. The max-targets attribute specifies the maximum number
    of targets against which a tool can run. The revision attribute
    allows a tool author to specified a revision for the tool. Note
    that this is for information only. The job-log attribute
    specifies whether the results of the command will be kept in this
    systems job log. When job-log="true" the job and target status
    for the tool will be kept for a relatively lengthy system-defined
    period in the database after the job completes. When
    job-log="false" only the last completed copy of the job and
    target status for the tool will be kept in the cache for a much
    shorter period of time, and will not be written to the database.
    Job logging is enabled by default. The schedulable attribute
    specifies whether the tool can be run as a scheduled task. When
    schedulable="false" the tool can only run as a "run now" task.
    Tools are schedulable by default. The guid attribute specifies a
    globally unique identifier (GUID) for the tool. Because the
    system generates a GUID for a tool during the add operation, this
    field should only be specified during a modify operation. -->
```

```
<!ATTLIST web-launch-tool name      CDATA #REQUIRED
    visible      (true | false) "true"
    max-targets  NMTOKEN #IMPLIED
    revision     NMTOKEN #IMPLIED
    job-log      (true | false) "true"
    schedulable (true | false) "true"
    guid         NMTOKEN #IMPLIED >
```

```
<!-- The web-block specifies the elements specific to a web launch
    tool. The web-block must specify a main-url element. Optionally,
    the web-block can specify a side-url element, a status-url
    element, and a current-url element. Additionally, the web-block
    can specify the parameters for the URLs. Finally, the web-block
    can optionally specify a target format to describe how targets
    are passed to a web launch aware tool. -->
```

```
<!ELEMENT web-block (main-url, (side-url?, status-url?, current-url?),
    parameter*, target-format? ) >
```

```
<!-- In addition to the above elements, the web-block element has one
      attribute. The accepts-targets attribute specifies whether the
      web launch tool accepts targets for execution. The
      accepts-targets attribute is true by default. -->

<!ATTLIST web-block accepts-targets (true|false) "true">

<!-- The main-url specifies the URL to launch the tool. If the URL
      accepts parameters, the URL must be specified as a parameterized
      string. -->

<!ELEMENT main-url ( #PCDATA ) >

      <!-- The status-url specifies a URL at which one might find the status
            of this web launch tool during execution. -->

<!ELEMENT status-url ( #PCDATA ) >

<!-- The current-url specifies the current URL. -->

<!ELEMENT current-url ( #PCDATA ) >

<!-- The side-url specifies a set-aside URL. -->

<!ELEMENT side-url ( #PCDATA ) >

<!-- The target-format defines the format of targets in a web launch
      tool and is specified as a parameterized string.-->

<!ELEMENT target-format ( #PCDATA ) >

<!-- The automation tool performs an action on the CMS which
      involves accessing the target systems. The automation-tool element
      can optionally specify a category element, a menu-category
      element, a description element, a comment element, an owner
      element, a default-target element, an execute-as-user element, a
      job-display-handler element, a default-parameter element, a
      role-enabled element, zero or more role elements, zero or more
      include-filter elements, or zero or more env-variable elements.
      If more than one of these elements are specified, the element
      must appear in the order as listed in this definition. The
      automation-tool element must contain an automation-block element.
      The automation-block element must appear after the previously
      described optional elements, if any of the optional elements are
      specified. Following the automation-block element, one can
      specify zero or more attribute elements. -->

<!ELEMENT automation-tool (category?, description?, comment?, owner?,
      default-target?, execute-as-user?,
      job-display-handler?,
      toolbox-enabled?, toolbox*,
      role-enabled?, role*,
      include-filter*, automation-block,
      attribute* ) >
```

```
<!-- In addition to the previously described elements, the
automation-tool element specifies the following attributes. The
name attribute specifies the tool name and must be specified in
the automation-tool element. The visible attribute specifies
whether the tool is visible for running. By default tools are
visible. The max-targets attribute specifies the maximum number
of targets against which a tool can run. The revision attribute
allows a tool author to specify a revision for the tool. Note
that this is for information only. The job-log attribute
specifies whether the results of the command will be kept in this
systems job log. When job-log="true" the job and target status
for the tool will be kept for a relatively lengthy system-defined
period in the database after the job completes. When
job-log="false" only the last completed copy of the job and
target status for the tool will be kept in the cache for a much
shorter period of time, and will not be written to the database.
Job logging is enabled by default. The schedulable attribute
specifies whether the tool can be run as a scheduled task. When
schedulable="false" the tool can only run as a "run now" task.
Tools are schedulable by default. The guid attribute specifies a
globally unique identifier (GUID) for the tool. Because the
system generates a GUID for a tool during the add operation, this
field should only be specified during a modify operation. The
accepts-targets attribute specifies whether the tool
accepts targets for execution. The accepts-targets attribute is
true by default. -->
```

```
!ATTLIST automation-tool name CDATA #REQUIRED
visible (true | false) "true"
max-targets NMTOKEN #IMPLIED
revision CDATA #IMPLIED
job-log (true | false) "true"
schedulable (true | false) "true"
guid NMTOKEN #IMPLIED
accepts-targets (true|false) "true" >
```

```
<!-- The automation-block specifies the elements specific to an
automation tool. The automation-block must specify a
message-id. -->
```

```
<!ELEMENT automation-block (message-id) >
```

```
<!-- The message-id is the internal string representation of the message
sent by the Automation engine to cause the tool to run. -->
```

```
<!ELEMENT message-id ( #PCDATA ) >
```

```
<!-- The app-launch-tool element specifies an application launch
tool. The app-launch-tool element can optionally specify a
category element, a menu-category element, a description element,
a comment element, an owner element, a default-target element, an
execute-as-user element, a job-display-handler element, a
default-parameter element, a role-enabled element, zero or more
```

role elements, zero or more include-filter elements, or zero or more env-variable elements. If more than one of these elements are specified, the element must appear in the order as listed in this definition. The app-launch-tool element must contain an app-launch-block element. The app-launch-block element must appear after the previously described optional elements, if any of the optional elements are specified. Following the app-launch-block element, one can specify zero or more attribute elements. -->

```
<!ELEMENT app-launch-tool (category?, description?, comment?, owner?,
    default-target?, execute-as-user?,
    job-display-handler?,
    role-enabled?, role*,
    toolbox-enabled?, toolbox*,
    include-filter*, env-variable*,
    app-launch-block, attribute* ) >
```

```
<!-- In addition to the previously described elements, the
    app-launch-tool element specifies the following attributes. The
    name attribute specifies the tool name and must be specified in
    the app-launch-tool element. The visible attribute specifies
    whether the tool is visible for running. By default tools are
    visible. The max-targets attribute specifies the maximum number
    of targets against which a tool can run. The revision attribute
    allows a tool author to specify a revision for the tool. Note
    that this is for information only. The job-log attribute
    specifies whether the results of the command will be kept in this
    systems job log. When job-log="true" the job and target status
    the tool will be kept for a relatively lengthy system-defined
    period in the database after the job completes. When
    job-log="false" only the last completed copy of the job and
    target status for the tool will be kept in the cache for a much
    shorter period of time, and will not be written to the database.
    Job logging is enabled by default. The schedulable attribute
    specifies whether the tool can be run as a scheduled task. When
    schedulable="false" the tool can only run as a "run now" task.
    Tools are schedulable by default. The guid attribute specifies a
    globally unique identifier (GUID) for the tool. Because the
    system generates a GUID for a tool during the add operation, this
    field should only be specified during a modify operation. The
    accepts-targets attribute specifies whether the tool
    accepts targets for execution. The accepts-targets attribute is
    true by default. -->
```

```
<!ATTLIST app-launch-tool name          CDATA    #REQUIRED
    visible      (true | false) "true"
    max-targets  NMTOKEN #IMPLIED
    revision     CDATA    #IMPLIED
    job-log      (true | false) "true"
    schedulable  (true | false) "true"
    guid         NMTOKEN #IMPLIED
    accepts-targets (true|false) "true" >
```

```
<!-- The app-launch-block specifies the elements specific to an
      application launch tool. The app-launch-block specifies a
      required command element. -->

<!ELEMENT app-launch-block (command, app-parameters?) >

<!-- In addition to the previously described elements, the
      app-launch-block element specifies the following attribute. The
      alert-driven attribute specifies whether the alert list or the
      system list is used to determine the target systems to run the tool
      on. -->

<!ATTLIST app-launch-block alert-driven (true | false) "false" >

<!-- The app-parameters element is an application parameters
      definition string whose value is a string -->

<!ELEMENT app-parameters ( #PCDATA ) >

<!-- The env-variable element is an environment variable definition
      string whose value is a string -->

<!ELEMENT env-variable ( #PCDATA ) >

<!-- In addition to the previously described elements, the
      env-variable element specifies the following attribute. The
      name attribute specifies the name of the environment variable.-->

<!ATTLIST env-variable name CDATA #REQUIRED >

<!-- The owner element specifies the tool owner. When the owner field
      is specified, the tool is only associated with the All Tools toolbox.
      When the owner field is not specified, tool is enabled in all
      of its associated toolboxes. When a limited-rights user adds or
      modifies a tool, the owner field contains the name of the
      limited-rights user. Only a full-rights user can add or modify a
      tool without the owner specified. -->

<!ELEMENT owner ( #PCDATA ) >

  !-- The comment field specifies additional information about the
      tool. It is usually more verbose than the description. -->

<!ELEMENT comment ( #PCDATA ) >

<!-- The parameter element specifies the first to the tenth parameter
      of a tool. -->

<!ELEMENT parameter EMPTY >

<!-- The parameter element has three attributes. The index attributes
      specifies which argument in a parameterized string this parameter
      substitutes. Parameters can be indexed from 1 to 10 with a
      default index of 1. Tools cannot contain parameters with
```

duplicate indexes. If more than one parameter in a tool definition contains the same index, only the first parameter added to the tool with the duplicate index remains in the tool. The prompt attribute provides information about the parameter that can be displayed in a GUI for assistance. The required attribute specifies whether this parameter must be specified when the tool is executed. By default, parameters are not required. The private attribute specifies whether this parameter is encoded and stored securely. By default, parameters are not private. -->

```
<!ATTLIST parameter index (1|2|3|4|5|6|7|8|9|10) "1"
  prompt CDATA #REQUIRED
  required (true|false) "false"
  private (true|false) "false" >
```

<!-- The toolbox-enabled element specifies whether the toolboxes associated with a tool are enabled. -->

```
<!ELEMENT toolbox-enabled EMPTY >
```

<!-- The toolbox-enabled element has one attribute. The value attribute specifies whether the tool within the toolboxes is enabled. This allows a full-rights user to explicitly disable the tools in a toolbox though the tool is always enabled in the All Tools toolbox. By default, the tool is enabled in all the toolboxes that it is in. If a tool is disabled within a toolbox, it cannot be executed. -->

```
<!ATTLIST toolbox-enabled value (true|false) "true">
```

<!-- The role-enabled element specifies whether the roles associated with a tool are enabled. This is an obsolete element. The toolbox-enabled element should be used instead.-->

```
<!ELEMENT role-enabled EMPTY >
```

<!-- See description of toolbox-enabled element attributes. -->

```
<!ATTLIST role-enabled value (true|false) "true">
```

<!-- The default-target element specifies a target on which the tool can run if no targets are specified at run time. One can specify a system, &cms2; to run on the &cms2; by default, or ALL to run on all authorized systems by default. -->

```
<!ELEMENT default-target ( #PCDATA ) >
```

<!-- The category element specifies the category with which to associate the tool. By default, tools are associated with the "Local Tools" category. -->

```
<!ELEMENT category ( #PCDATA ) >
```

<!-- The description element specifies a simple description of the tool. To specify more verbose information such as how to run the

```
    tool, use the comment element. -->

<!ELEMENT description ( #PCDATA ) >

<!-- For SSA and MSA command tools, the execute-as-user element
    specifies the user name that the tool runs as or under whose
    account the tool runs on the target systems. For Web-launch
    tools the execute-as-user is passed to the URL for its use. -->

<!ELEMENT execute-as-user ( #PCDATA ) >

<!-- The job display handler element specifies the fully-qualified
    name of a class implementing the JobDisplayHandler interface,
    used to display the results of a job created by running this
    tool. -->

<!ELEMENT job-display-handler ( #PCDATA ) >

<!-- The toolbox element specifies a toolbox to associate with the
    tool. To run a tool the user must be authorized with one of the
    specified toolboxes. -->

<!ELEMENT toolbox EMPTY >

<!-- The toolbox element has one attribute to specify the toolbox
    name. -->

<!ATTLIST toolbox toolbox-name CDATA #REQUIRED >

<!-- The role element specifies a role to associate with the tool. To
    run a tool the user must be authorized with one of the specified
    roles. This element is obsolete. The toolbox element should be
    used instead. -->

<!ELEMENT role EMPTY >

<!-- See the toolbox element attribute description. -->

<!ATTLIST role role-name CDATA #REQUIRED >

<!-- The include-filter element specifies system attributes against
    which to filter a tool for execution. A specified include-filter
    element must contain one or more system-filter elements. When
    filtering a tool each include-filter block is OR'd together to
    get the final filter result. Each system-filter element within an
    include-filter block is AND'd together. -->

<!ELEMENT include-filter (system-filter)+ >

<!-- The include-filter elements has one attribute. The type attribute
    specifies the type of include filter to execute. Four types are
    currently recognized. Three of them are os (operating system),
    hardware, protocol filtering. The fourth type is called other which
    will allow all other system attributes to be filtered upon.-->
```

```
<!ATTLIST include-filter type (os | hardware | protocol | other) "os" >

<!-- The system-filter element is an empty element that contains
      attributes used to specify the system attributes against which to
      filter a tool for execution. -->

<!ELEMENT system-filter EMPTY >

<!-- The system-filter element is specified with three attributes. The
      name attribute specifies the system attribute name to filter
      against. The operator attribute specifies whether to filter
      against an equal value, a less than value, a greater than or
      equal value, a contains value, a not equals value or a not
      contains value. The operator name is case-insensitive. The
      value attribute specifies the value of the system attribute to
      filter against. -->

<!ATTLIST system-filter name CDATA #REQUIRED
      operator (EQ | GE | LT | CT | NEQ | NCT |
      eq | ge | lt | ct | neq | nct |
      Eq | Ge | Lt | Ct | Neq | Nct |
      eQ | gE | lT | cT | nEQ | nCT ) "EQ"
      value CDATA #REQUIRED >

<!-- The attribute element specifies the name value pairs that
      comprise client attributes. The client attribute name is
      specified using the name attribute and the client attribute value
      is specified as the PCDATA of the element. -->

<!ELEMENT attribute ( #PCDATA ) >

<!ATTLIST attribute name CDATA #REQUIRED >
```

Related Procedures

- New Command Line Tool
- New Copy a File Tool
- Removing and Restoring Tools
- New Web Launch Tool
- New X Window Tool

Related Topic

- Command Line Tools

Examples of Using Parameter Strings in Command Line Tools

The URL strings for Web aware tools and command line tools must be provided as absolute URLs beginning with `http://` or `https://`. For example,

```
https://%n:1188/kcweb/ https://%l:2381/
```

Web Launch Aware tools and command line tools that always run on the central management server (CMS) must be relative URLs beginning with `/`. For example,

```
/propertypages/Identify.jsp?device=%n
```

Multiple selections can be substituted into the URL. A selection index is used during the substitution process to keep track of the *current* selection. The selection index is initially set to one, and the first selection of the list of selected target systems remains current until a `%z` parameter is encountered in the URL (an exception to this exists in the repeat block, discussed later), at which time the next selection becomes current and the selection index is incremented by one, and so on. For example,

```
http://server/app/doit.jsp?name=%n%z&addr=%a
```

where the `doit.jsp` page is invoked with the network name of the first selected system assigned to the `name` parameter and the IP address of the second selected target assigned to the `addr` parameter.

Any number of selected targets can be substituted by using the repeat block construct, `%(... %)`. Anything inside the repeat block delimiters is repeated until the selection list is exhausted, starting with what is then the current selection and selection index. For example,

```
https://%{deploy.server%}/deploy/deployimage.jsp?
device1=%n%z%(&device%i=%n%z%)
```

Note:



The use of the `%i` parameter. The current selection index (1,2,3,and so on) is substituted for this parameter during the substitution process.

Note:



If the end of the repetition clause is reached and no `%z` parameter has been encountered, then the selection index and current election are automatically incremented to avoid an infinite loop during the substitution phase.

If we have two selected target systems in the above example, the expanded URL string would look like:

```
https://deploy.hp.com:280/deploy/deployimage.jsp?
device1=nodea.hp.com&device2=nodeb.hp.com
```

If we have only 1 selected target system in the above example, the expanded URL string would look like:

```
https://deploy.hp.com:280/deploy/deployimage.jsp? device1=nodea.hp.com
```

Since there is no current selection when we get to the repeat block, the entire repeat block is suppressed during the substitution process.

Related Procedures

- New Command Line Tool
- New Copy a File Tool
- New Web Launch Tool
- New X Window Tool
- Removing and Restoring Tools

Related Topics

- Command Line Tools
- Creating New Command Line Tools

Custom Commands

Custom commands are executed on the central management server (CMS) and not on target systems, and are intended to be scripts, batch files, or executables that can reference environment variables set by the tool in order to access system or event information. For example, creating a custom command to launch Notepad.

Custom commands require the use of environment variables which are parameters passed to the launched application to make it perform as expected. Refer to “Environment Variables for Custom Commands” for more information. The launch command string includes system variables and user-defined variables for your application. For example, you could pass an environment variable that runs a script to check on the status of your mail server.

Note:



DOS environment variables are supported in the custom command parameters and work as parameters on the **New Custom Command** page or the **Manage Custom Commands** page. However, they must be surrounded by double % signs. For example, to pass in the `NOTICELABEL` environment variable as a parameter, it should be entered as `%%NOTICELABEL%%` on the parameter line. The environment variables can also be accessed from a batch file or script file. To use them in a batch file or a script file, only a single % sign should precede and succeed the environment variable name. Refer to [Command Line Tools - Parameterized Strings Substitution Table \[useTools_commandLineTools_ref.html#SubstitutionTable\]](#) for a list of other substitutable variables.

Custom commands that you create are displayed under the **Tools->Custom Commands** menu option.

You have multiple scheduling options. Refer to “Scheduling a Task” for more information about scheduling options.

Important:



The application must be able to execute in the security context provided to HP Systems Insight Manager (HP SIM) (the default is LocalSystem).

- **New Custom Commands.** Select **Tools>Custom Commands>New Custom Commands**. The **New Custom Commands** page appears.
- **Manage Custom Commands.** Select **Tools>Custom Commands>Manage Custom Commands**. The **Manage Custom Commands** page appears.
- **New Web Launch Tool.** Select **Tools>Custom Commands>New Web Launch Tool**. The **New Web Launch Tool** page appears. This tool is for Linux and HP-UX systems only.
- **Remove a Tool.** Select **Options>Remove a Tool**. The **Remove a Tool** page appears.

Related Procedures

- Creating a New Custom Command
- Managing Custom Commands

Related Topic

- Environment Variables for Custom Commands

Creating a New Custom Command

Use the New Custom Commands to launch an application on the server that is running HP Systems Insight Manager (HP SIM).

To create a custom command:

1. Select **Tools>Custom Commands>New Custom Command**. The **New Custom Command** page appears.
2. In the **Name** field, enter the command name.

Important: Custom command names must be at least one character in length, and no more than 255 characters in length. The first character of the name must be alphabetic. Characters following the first character can be letters, digits, spaces, or any of the following characters: "-", ".", "(", ")", or "_".

3. In the **Description** field, enter the necessary information for this application.
4. In the **Comments** field, enter any comments for this application.
5. In the **Command (Executable path and file name)** field, enter the full path (from the root of the HP SIM console) and the file name of the application. For example:

`c:\custom code\romflash.bat`

- In the **Parameters** field, enter the necessary command line parameters for this application.

Parameter substitution is supported as defined in Parameterized Strings. Refer to “Parameterized Strings” for more information.
- Enter the **Variable name** and **Value** for the **Environment variables**. Click **Add** after you enter each set of variables and values. To clear a previously set variable, highlight the variable, and click **Delete**. Refer to “Environment Variables for Custom Commands” for information on environment variables.

Note: DOS environment variables are supported in the custom command parameters and work as parameters on the **New Custom Command** page or the **Manage Custom Commands** page. However, they must be surrounded by double % signs. For example, to pass in the *NOTICELABEL* environment variable as a parameter, it should be entered as `%%NOTICELABEL%%` on the parameter line. The environment variables can also be accessed from a batch file or script file. To use them in a batch file or a script file, only a single % sign should precede and succeed the environment variable name. Refer to Command Line Tools - Parameterized Strings Substitution Table [[useTools_commandLineTools_ref.html#SubstitutionTable](#)] for a list of other substitutable variables.
- After you finish entering the custom command information, click **OK**. The new command is added to the **Custom Commands** menu.

Note:



New custom command tools are located under **Tools->Custom Commands->Application Launch Tools**.

Related Procedure

- Managing Custom Commands

Related Topic

- Custom Commands

Managing Custom Commands

The **Manage Custom Commands** page displays all the custom command tools created. It displays tool names, descriptions, commands, and parameters. To view all the tools created, select **Tools->Custom Commands->Manage Custom Tools**.

The following options are available for managing custom commands:

- “New”
- “Edit”

- “Run Now/Schedule”
- “Delete”

New

To create a new command, select **New**. Refer to “Creating a New Custom Command” for more information.

Edit

To edit a command, select the command and click **Edit**. The **Edit Custom Command Details** section appears. All fields can be edited, and environment variables can be added and deleted. To save changes, click **OK**. To discard the changes, click **Cancel**.

Run Now/Schedule

To run a tool, select the tool to run immediately or schedule and click **Run Now/Schedule**.

Refer to “Scheduling a Task” or “Running a Scheduled Task” for more information.

Delete

Select the command to be deleted. Deleting a command removes it from the **Manage Custom Commands** page and from the system.

Note:



If a command being deleted is dependent on a task, an alert displays with the list of tasks associated with the command.

Related Procedure

- Creating a New Custom Command

Related Topic

- Custom Commands

Editing a Custom Command

You can edit any existing custom commands by selecting a command from the **Managing Custom Commands** page. All fields are editable.

To edit an existing custom command:

1. Select **Tools->Custom Commands->Manage Custom Commands**. The **Manage Custom Commands** page appears.

2. Select the custom command that you want to edit and click **Edit**. The **Edit Custom Command** section appears.
3. In the **Name** field, enter the command name.

Important: Custom command names must be at least one character in length, and no more than 255 characters in length. The first character of the name must be alphabetic. Characters following the first character can be letters, digits, spaces, or any of the following characters: "-", ".", "(", ")" or "_".

4. In the **Description** field, enter the necessary information for this application.
5. In the **Comments** field, enter any comments for this application.
6. In the **Command (Executable path and file name)** field, enter the full path (from the root of the HP SIM console) and the file name of the application. For example:

```
c:\custom code\romflash.bat
```

7. In the **Parameters** field, enter the necessary command line parameters for this application.
Parameter substitution is supported as defined in Parameterized Strings. Refer to "Parameterized Strings" for more information.
8. Enter the **Variable name** and **Value** for the **Environment variables**. Click **Add** after you enter each set of variables and values. To clear a previously set variable, highlight the variable, and click **Delete**. Refer to "Environment Variables for Custom Commands" for information on environment variables.

Note: DOS environment variables are supported in the custom command parameters and work as parameters on the **New Custom Command** page or the **Manage Custom Commands** page. However, they must be surrounded by double % signs. For example, to pass in the *NOTICELABEL* environment variable as a parameter, it should be entered as *%%NOTICELABEL%%* on the parameter line. The environment variables can also be accessed from a batch file or script file. To use them in a batch file or a script file, only a single % sign should precede and succeed the environment variable name. Refer to Command Line Tools - Parameterized Strings Substitution Table [useTools_commandLineTools_ref.html#SubstitutionTable] for a list of other substitutable variables.

9. After you finish entering the custom command information, click **OK**. The new command is added to the **Custom Commands** menu.

Note:



New custom command tools are located under **Tools->Custom Commands->Application Launch Tools**.

Related Procedure

- Managing Custom Commands

Related Topic

- Custom Commands

Environment Variables for Custom Commands

Note:



If your user-defined variables have the same names as the HP Systems Insight Manager (HP SIM) environment variables, the HP SIM environment variables override the user-defined variables.

NOTICELABEL. Type of notice; a small string that contains Discovered System, other HP SIM server-level notices, or the type of trap that caused the notice

NOTICESTATE. Internal value used by HP SIM, indicating whether the notice is cleared

NOTICEPLAINTEXT. Plain text description of the notice that contains detailed information about the notice (In Progress, Cleared, or Not Cleared)

NOTICERAWDATA. The raw data from the notice is passed as a string; this is a small pipe (|) delimited set of variables and might be useful for some simple parsing rules

NOTICESEVERITYSTR. Verbose description of the notice severity that can be one of Critical, Informational, Major, Minor, Unknown, Warning, and Normal

NOTICESEVERITY. Integer value of the *NOTICESEVERITYSTR* that can be one of:

- 0, Unknown
- 1, Normal
- 2, Warning
- 3, Minor
- 4, Major
- 5, Critical
- 100, Informational

NOTICEQUERYNAME. Displays the collection name based on how the notice was generated; this value can say one of the following:

- This system or event meets the following search criteria: +QueryName;
- This system or event now meets the following search criteria:
+QueryName;
- This system or event no longer meets the following search criteria:
+QueryName;

DEVICENAME. Name of the system that caused the notice

DEVICEIPXADDRESSCOUNT. Number of IPX addresses that are mapped to this system

DEVICEIPADDRESSCOUNT. Number of IP addresses that are mapped to this system

DEVICEIPADDRESS%d. Based on the count, %d is an integer that shows the actual IP address, for example:

```
IF, DEVICEIPADDRESSCOUNT = 2
```

```
Then, DEVICEIPADDRESS0 = 111.111.111.111
```

```
DEVICEIPADDRESS1 = 222.222.222.222
```

DEVICEIPXADDRESS%d. Based on the count, %d is an integer that references the actual IPX address

DEVICEMACADDRESSCOUNT. Number of MAC addresses collected for the system (a Data Collection Task must be run before this information is available)

DEVICEMACADDRESS%d. Based on the MAC address count, %d is an integer that references the actual MAC address environment variable, for example:

```
IF, DEVICEMACADDRESSCOUNT = 2
```

```
Then, DEVICEMACADDRESS0=00:80:5F:7F:B0:81
```

```
DEVICEMACADDRESS1=00:80:C7:29:EF:B6
```

GENERICTRAPID. Set to the SNMP Generic Trap ID of the trap received if this is an event-based list and originated from an SNMP trap

SPECIFICTRAPID. Set to the SNMP Specific Trap ID of the trap received if this is an event-based list and originated from an SNMP trap

Path. Has the Path environment variable value from the context in which the service is running

SystemRoot. Has the SystemRoot environment variable value from the context in which the service is running

Windir. Has the Windir environment variable value from the context in which the service is running

COMPUTERNAME. Has the COMPUTERNAME environment variable value from the context in which the service is running

MPIP. This environment variable returns the IP address of the associated management processor.

MPNAME. This environment variable returns the name of the associated management processor.

RELATEDDEVICECOUNT. This environment variable returns the count of how many associated devices are there.

RELATEDDEVICENAME%d. This environment variable returns the name of the associated device where %d is the iteration number, for example:

```
IF, RELATEDDEVICECOUNT = 2
```

Then, RELATEDDEVICENAME0=DeviceName0

RELATEDDEVICENAME1=DeviceName1

RELATEDDEVICEIP%d. This environment variable returns the IPaddress of the associated device where %d is the iteration number, for example:

IF, RELATEDDEVICECOUNT = 2

Then, RELATEDDEVICEIP0=111.111.111.111

RELATEDDEVICEIP1=222.222.222.222

RELATIONSHIP%d. This environment variable returns the relationship string with the associated device and %d is the iteration number.

IF, RELATEDDEVICECOUNT = 2

Then, RELATIONSHIP0=ServerToEnclosure

RELATIONSHIP1=VMGuestToVMHost

Related Procedures

- Managing Custom Commands
- Creating a New Custom Command

Related Topic

- Custom Commands

New Web Launch Tool

Note:



This tool is available on Linux and HP-UX systems only.

Use this tool to create a tool that integrates a Web application or website. All tools are automatically launched into a separate window. For example, to add a path to HP's website, add the URL: `http://hp.com`. To add a link to the site on a selected system, enter **Yes** under **Accepts a target selection ...**, then add a URL, such as: `https://%n:2381`. The target system is substituted for the %n when the tool is launched. The resulting command launches the System Management Homepage on the target system. This tool creates a temporary XML tool definition file under `/var/tmp` then loads it with the command `mxttool -af file`. You only need to enter data into the required fields.

To create a new Web launch tool:

1. Select **Tools->Custom Commands->New Web Launch Tool**. The **New Web Launch Tool** page appears.

2. Under **Parameters**, add information using the standard tool parameters. The following fields are required:
 - Tool name
 - URL to the site or application to launch
 - Selects a target selection % (yes or no)
3. Click **Run Now** to run the task immediately or **Schedule** to schedule when the task runs. Refer to “Scheduling a Task” for more information on scheduling a task.

Additional Information

Additional information is available in the following sections:

- “Tool Types”
- Command Line Tools - Parameterized Strings Substitution Table [useTools_commandLineTools_ref.html#SubstitutionTable]
- “Tool Filtering”
- “Version Numbers”
- “Other Requirements”
- “Document Type Definition”

Related Procedures

- Creating a New Custom Command
- Managing Custom Commands
- New Command Line Tool
- New Copy a File Tool
- Removing and Restoring Tools
- New X Window Tool

Related Topics

- Custom Commands
- Environment Variables for Custom Commands
- Command Line Tools
- Command Line Tools Reference
- Examples of Using Parameter Strings in Command Line Tools

Configuring DMI Access

The **Configure->DMI Access** tool allows setting the HP Systems Insight Manager (HP SIM) central management server (CMS) as the event target on selected HP-UX systems where DMI has been installed. This adds the HP SIM CMS server name to `/var/dmi/dmiMachines` on each selected system.

Related Procedure

- Configuring SNMP Access

Configuring SNMP Access

The **Configure->SNMP Access** tool allows setting the HP Systems Insight Manager (HP SIM) central management server (CMS) as the trap target on selected HP-UX systems. This adds the HP SIM CMS server name to `/etc/SnmpAgent.d/snmpd.conf` on each selected system.

To configure SNMP to send traps to the CMS:

1. Add the full hostname or IP address of the CMS as a trapdest in the file `/etc/SnmpAgent.d/snmpd.conf`:

```
trap-dest: hostname_or_ip_address
```

2. Stop the SNMP Master agent and all subagents with the command:

```
/sbin/init.d/SnmpMaster stop
```

3. Restart the SNMP Master agent and all subagents with the command:

```
/usr/sbin/snmpd
```

Related Procedure

- Configuring DMI Access

Device Ping

Use the Ping tool to ping an individual system or multiple systems. To ping systems, select **Diagnose->Ping**. The **Ping** window appears. Select the target systems and click **Run Now** to run the task. Refer to “Creating a Task” for more information.

If a system does not have an IP or IPX address, the request cannot be performed. For systems with multiple IP or IPX addresses, the result of each IP address occupies one row in the result page. The status on the upper right corner displays: `Pinging selected systems`. After all the systems on the list have been pinged, the status displays: `Ping completed` with a time stamp of the completion time.

The ping results are displayed in a separate window. The following are the replies that you might receive:

- `Replied`. The request has been executed successfully, and the pinged system has responded.
- `Request timed out`. The request has been executed, but the pinged system failed to respond.
- `System has no IP/IPX address`. There is no IP or IPX address associated with the system. `Unable to perform ping`.
- `No system is selected`. No system is selected.

If the ping is successful, there is no retry. You can only retry when the ping fails. The ping results have no effect on the system status on the **Task Results** or system view pages.

Disk Thresholds

Setting Disk Thresholds

Setting disk thresholds is a task you can perform in HP Systems Insight Manager (HP SIM). Use this task to set a disk threshold for systems in an associated list. This threshold is set on all disk volumes on the target system.

To set disk thresholds, select **Configure>Disk Thresholds>Set Disk Thresholds**. The **Set Disk Thresholds** window appears. To select target systems, refer to “Creating a Task”, and to specify the disk thresholds settings, refer to “Setting Disk Thresholds” for more information.

Follow these guidelines for setting thresholds:

- When you save the thresholds, disabled thresholds are deleted. A **Critical Disk Percent Usage Threshold** can never go above 99% or lower than a warning threshold plus 3%. Therefore, if the warning threshold is 85%, the valid range for the critical threshold is 88% to 99%.
- A **Reset Critical Disk Percent Usage Threshold** must drop below the reset value before the threshold is rearmed. This setting prevents the threshold from being sent multiple times if the variable fluctuates near the threshold value.
- The **Warning Disk Percent Usage Threshold** should be less than the critical threshold. A warning threshold must drop below the reset value before the warning threshold is rearmed. This setting prevents the threshold from being sent multiple times if the variable fluctuates near the threshold value. The minimum difference between the value and the reset value must be greater than or equal to 2%.
- When you save the thresholds, disabled thresholds are deleted. A **Reset Warning Disk Percent Usage Threshold** can never be higher than the critical threshold minus 3%. For example, if the critical threshold is 95%, the valid range for the warning threshold is 6% to 92%.
- The **Agent Polling Interval** value is the polling interval in seconds that determines how often the agents check if the current values exceed the threshold. A common value is 120 seconds.

Removing Disk Thresholds

Removing disk thresholds is another task that you can perform in HP SIM. Use this task to remove disk thresholds from systems in an associated list. This task only removes disk thresholds that were set by HP SIM or by browsing directly to the HP Insight Management Agent. Any thresholds set by Insight Manager (WIN32), including disk thresholds, are not removed by this task.

To remove disk thresholds, select **Configure>Disk Thresholds>Remove All Disk Thresholds**. The **Remove All Disk Thresholds** window appears. To select target systems, refer to “Creating a Task” for more information. After the target systems are selected, click **Schedule** to schedule when the task will run, or click **Run Now** to run the task immediately. The **All Scheduled Tasks** page appears.

Related Procedures

- Setting Disk Thresholds
- Scheduling a Task

Setting Disk Thresholds

You can create a systems list to use with this task, specifying system characteristics, or use existing system lists. Specify the disk thresholds to be set on supported systems.

To set disk thresholds:

1. Select **Configure**>**Disk Thresholds**>**Set Disk Thresholds**. The **Set Disk Thresholds** page appears.
2. Select target systems and click **Next**. Refer to “Creating a Task” for more information.
3. In the **Specify the disk thresholds to be set on supported systems** section, enter the following information:
 - Critical disk percent usage threshold (percent)
 - Reset critical disk percent usage threshold at (percent)
 - Warning disk usage threshold (percent)
 - Reset warning disk usage threshold at (percent)
 - Agent polling interval (seconds)Refer to “Disk Thresholds” for guidelines on setting these parameters.
4. Click **Previous** to return to the previous page. Click **Schedule** to schedule when the task runs. Refer to “Scheduling a Task” for more information on scheduling the task. Or click **Run Now** to run the task immediately. The **Task Results** page appears.

Related Procedures

- Creating a Task
- Scheduling a Task

Related Topic

- Disk Thresholds

Creating a Task to Delete Disk Thresholds on a Monthly Basis

The following example describes the necessary steps to set up a task that removes all disk thresholds on a monthly basis from the HP Systems Insight Manager (HP SIM) database.

Creating the Task

1. Select **Configure>Disk Thresholds>Remove All Disk Thresholds**. The **Remove All Disk Thresholds** page appears.
2. Select **All Servers** from the **Add targets by selecting** dropdown list.
3. Select the **Select "All Servers" itself** checkbox.
4. Click **Apply**.
5. Click **Schedule**.
6. In the **Task name** field, enter a name for the task, such as **Delete Disk Thresholds Monthly**.
7. Under **When would you like this task to run?** section, select **Periodically**.
8. In the **Refine schedule** section, select every month and select a day for the task to run.
9. Click **Done**.

Related Procedures

- Setting Disk Thresholds
- Creating a Task
- Scheduling a Task
- Running a Scheduled Task

Related Topic

- Disk Thresholds

License Manager

License Manager provides support for ProLiant Essentials based licensing. This support includes license key distribution, reconciliation, and reporting.

Note:



To run License Manager, a user must be given full-configuration-rights on the central management server (CMS) (to set, select **Options>Security>Users and Authorizations>User**) and the **All Tools** toolbox (to set, select **Options>Security>Users and Authorizations>Authorizations**).

Refer to "Users and User Groups" and "Toolboxes" for more information.

License keys can be collected and deployed to and from specified target systems known to HP Systems Insight Manager (HP SIM). For some products, the keys are sent to the specified system, while for other products, the licensing information is simply updated in the License Manager database. The license key database can be reviewed. New keys can be added individually or added in bulk from a file. License Manager also displays license information on Integrated Lights-Out

(iLO) systems, which is collected automatically. License Manager cannot deploy keys to an iLO. Keys deployed to the iLO host machine are not recognized by the iLO.

The Licensing menu provides you with the following options:

- **Managing Keys.** Select **Deploy->License Manager->Manage Keys**. This action displays the license keys and their assignments as known to License Manager and offers the facility to add keys, individually or in bulk, and view details on the use of a specific key.
- **Collecting Keys.** Select **Deploy->License Manager->Collect Keys**. Selects one or more target systems from which to collect keys. Refer to “Creating a Task” for more information on selecting targets.
- **Deploying Keys.** Select **Deploy->License Manager->Deploy Keys**. Selects one or more target systems to receive keys, and one or more license keys from the License Manager database to deploy. Refer to “Creating a Task” for more information on selecting targets. Select one or more keys to deploy. iLO keys are not included because there is no mechanism to deliver the key to the iLO.

License Manager Deploy Key and Collect key functions operate directly on the License Manager database or in the Windows registry on the target system depending on the product. Apart from early versions of HP ProLiant Essentials Performance Management Pack (PMP), all key information for HP SIM plug-ins is maintained by License Manager in the HP SIM database. For some products, the key must be kept in a licensing structure in the Windows registry on the licensed system. License Manager employs DCOM to deploy keys to and collect keys from those remote systems. Current versions of PMP require the keys to be in the Windows registry of the CMS. Keys for PMP must always be deployed or collected from the CMS system ONLY.

Authentication credentials for the specified systems are needed only in those situations where keys are being sent to the specified system. If WBEM authentication credentials have been provided for a specific target, these credentials are used. Refer to “Setting Protocols for a System or Groups of Systems” for more information. If specific credentials have not been provided, each set of Web-Based Enterprise Services (WBEM) credentials provided as global credentials are used in turn. Refer to “Setting Global Protocols” for more information. If no credentials are provided, the connection is attempted using the default credentials of the HP SIM server. The remote registry service must be started and running on candidate target systems for key collection or deployment.

Related Procedures

- Collecting Keys
- Deploying Keys
- Managing Keys
- Configuring Automatic Discovery

Related Topics

- System License Information Reporting
- About Keys

About Keys

License keys are encoded to authorize use of up to three different products and consequently, the same key might appear up to three separate times in the database assigned to the same system,

once for each product licensed by that key. The number of seats permitted by the key are applied in full to each product authorized by the key. A key authorizing five seats and two products authorizes five seats for each of the two products.

Eight types of licenses are available:

- **Free Flexible Quantity.** ProLiant Essentials products can optionally ship with one free, permanent license. This key type is the embodiment of that free license. The number of seats permitted by this license depends on the product and the product team. Keys of this type cannot be entered by the user into the License Manager database. The product alone can insert these keys into the database.
- **Flexible Quantity.** This license offers full, unlimited functionality for an unlimited time and for a specific number of seats purchased, up to 50,000.
- **Activation Key Agreement.** This license offers full, unlimited functionality for an unlimited time. This license represents an expected upper limit on the number of seats, up to 50,000.
- **Demo (seats and time).** This license offers full, unlimited functionality for a limited time and a specific number of seats. The license determines the number of days the key allows the product to function. The days begin counting from the day of first use. The key can permit more than one instance of the product to run. Demo keys can authorize up to 255 seats for up to 255 days.
- **Demo.** This license offers full, unlimited functionality for a limited time. The license determines the number of days the key allows the product to function. The days begin counting from the day of first use. The key can permit more than one instance of the product to run. Demo keys can authorize use for up to 65535 days.
- **Evaluation.** This license offers full, unlimited functionality and is distributed only in special circumstances.
- **Individual.** This license offers full, unlimited functionality and represents a single-use key for the Integrated Lights-Out (iLO) product.
- **Subscription.** This license is a time limited full functionality license. This key can indicate unlimited use for a specified period of time or a limited number of seats for that same period of time.
- **Intrinsic.** This license offers full, unlimited functionality and represents a single-use key for the Integrated Lights-Out (iLO) product.

Related Procedures

- License Manager
- Collecting Keys
- Managing Keys

Related Topics

- Viewing Key Database Contents
- Viewing Key Details

Collecting Keys

The Collect Keys feature collects license keys from selected systems. If the keys are stored directly on the selected system (refer to the specific product information for details), the central management server (CMS) and the selected machine must be running a variant of Microsoft Windows operating systems. Many products (mostly HP Systems Insight Manager (HP SIM) plug-ins) now save their key information in the License Manager database only. In these instances, there are no restrictions on the operating system of the CMS or selected system. The status line advises when a key should be collected from a remote selected system and that is not possible under the current circumstance.

Select **Deploy->License Manager->Collect Keys**. The **Collect Keys** window appears.

Related Topics

- License Manager
- Deploying Keys
- Managing Keys

Collect Keys Results

The Collection Results page appears with the following:

- **System Name.** This column displays the names of the systems on which the task was executed.
- **Key.** This column displays the keys received from the target system. There is one row for each system, key, and product retrieved from that system.
- **Product.** This column displays the name of the product associated with the use of this key.
- **Response Status.** This column displays the response status of the system. If the Collect Keys task was successful, a message appears, indicating the key collected successfully.

If there was an error, an error message appears. Error messages include:

If the local operating system and the remote selected system are not running Windows and License Manager is attempting to collect key information from the selected system directly, the following message is included: Cannot collect keys stored directly on this node. HP Systems Insight Manager host and specified system must be running Microsoft Windows.

- No licensing information found for this system.
- There are no keys for this node maintained by HP Systems Insight Manager (HP SIM) locally.
- Cannot collect keys stored directly on this node. HP SIM host and specified system must both be running Microsoft Windows.
- Target system denied connection access. Provide WBEM access credentials for this system.
- Credentials invalid or conflict with an existing set in use or the trust relationship between domains has failed or referenced IPC\$ account is locked out. There is a conflict between the credentials supplied and those

used in a current connection with the target system. Alternatively, the credentials supplied are outside of the domain the target is operating within.

- Keys cannot be collected from this system. There are no products for a system of this type. The target selected is not a server, desktop, notebook, or other type of like system.

The following error messages indicate that a problem with License Manager has occurred at the target system:

Note: The following errors are very rare.

- Licensing information error on target system. The key information found at the target contains errors in format or in some other detail.
- Problem collecting licensing information. The collection process failed for this target. The system might be offline such as powered down or disconnected from the network.
- Failed to contact this system. Network path not found or similar error. This system did not respond to the request for licensing information. The system might be offline such as powered down or disconnected from the network.
- Specified system is no longer in the database. The system information in the HP SIM database has been deleted by some other process.
- Target node list is empty. The list of target system names to collect keys from is not empty. A conflict with another user deleting the same systems from the database is likely.

Related Topics

- License Manager
- Collecting Keys
- Deploying Keys
- Managing Keys

Deploying Keys

The Deploy Keys feature deploys license keys to the selected systems. For some products which require their keys to be stored outside of the HP Systems Insight Manager (HP SIM) License Manager, both the central management server (CMS) and selected system operating system must be running Windows of some type. Otherwise, there are no restrictions. Deploy advises when there is a conflict.

To access the Deploy Keys:

1. Select **Deploy>License Manager>Deploy Keys**. The **Deploy Keys** window appears.
2. Select one or more target systems to deploy to and one or more license keys from the License Manager database to deploy. Refer to "Creating a Task" for more information on selecting targets. Current versions of HP ProLiant Essentials Performance Management Pack (PMP) require all keys to be deployed on the CMS.
3. Click **Next**.

Related Topics

- License Manager
- Selecting Keys
- Deploy Key Results
- About Keys

Selecting Keys

1. The Select keys to deploy section only offers keys that are suitable and are not fully consumed. For example, a key with free seats or a BETA key that has not yet expired. Integrated Lights-Out (iLO) keys are not included. The key selection table appears with the following columns:
 - **Product.** The name of the licensed product.
 - **Version.** The version of the software for which the license is valid. Higher versions support lower versions, but lower versions do not support higher versions. For example, version 2 would support version 1 software, but version 1 would not support version 2 software.
 - **License Type.** Six types of licenses are available (refer to “About Keys” for more information.)
 - **Seats Max.** The total number of licenses authorized for use by this key.
 - **Seats Used.** The number of licenses that are currently used.
 - **Days Max.** The total number of days authorized for use by this key (time-specific keys only), but for BETA key type, this is the number of days from the date the key was issued. For all others, it is the number of days from when the key was first used.
 - **Key string.** The license key.
2. Click **Run Now**. Select another action from the menu to abort the deploy operation.

Note:



The list of keys offered does not include:

- Keys for Integrated Lights-Out (iLO)
 - Specific keys that are fully subscribed
-

Related Topics

- Deploy Key Results
- License Manager
- Deploy Key Results
- Collecting Keys
- Managing Keys

Deploy Key Results

The following information displays on the **Deployment Results** page:

Some keys can authorize use of one, two, or three different products, and therefore, one key can be deployed up to three times, once for each product it authorizes. The user cannot specify which product, authorized by a key, is to be deployed. The key is deployed and enables all of the products it licenses. If a product is not used on that system, no authorizations of use are consumed, and the user takes no penalty as a result. Although License Manager displays information on Integrated Lights-Out (iLO) systems, licensing keys cannot be deployed directly to iLO systems because these systems do not currently support key deployment using this tool.

Note:



In some instances where the key must be physically delivered to the selected system and the central management server (CMS) or the selected system is not running Windows, the following status message appears: Cannot deploy this key. HP Systems Insight Manager (HP SIM) host and specified system must be running Microsoft Windows to deploy a key for this product.

Note: There is one row per system, per key, and per product for each key deployment of a key.

- **System Name.** This column displays the names of the systems on which the task was executed.
- **Key.** This column displays the key deployed to the target system.
- **Product.** This is the name of the product associated with the deployment of this key.
- **Response Status.** This column displays the response status from the system. If the Deploy Key task was successful for a specific target system and key, the `The key deployed successfully` message displays.

If the Deploy Key task failed, an error message appears.

Possible error messages when the key must be sent to the selected system directly, include:

- `Target system is not running Microsoft Windows as required. The target node must be running some variant of the Windows operating system.`
- `Target system denied connection access. Provide WBEM access credentials for this system. The default or supplied credentials are invalid for access to this target.`
- `Credentials supplied are invalid or conflict with an existing set in use or the trust relationship between domains has failed. There is a conflict between the credentials supplied and those used in a current connection with the target system. Alternatively, the credentials supplied are outside of the domain (or trust) within which the target is operating.`
- `Keys cannot be deployed to this system. There are no products for a system of this type. The target is not a server, desktop, notebook, or other suitable system.`

- Permission to write licensing information at target system denied. The target system is not permitting remote access to its registry. The “remote registry service” must be running on all candidate targets. In this case, a simple check might help.
 - `telnet hostname` (connect to target host)
 - `net start` (verify that the remote registry service is already running)
 - `net start remote registry service` (start registry service if needed)

Note: The following errors are possible in any deployment situation, but are rare.

- Specified system is no longer in the database. The node information in the HP SIM database has been deleted by some other process.
- Failed to create certificate for this key. There is a problem installing the key on this target system. It might be necessary to apply the key directly to the application or system requiring it.
- Deployment of a key of this format is not supported. Key deployment is intended to support ProLiant Essentials keys only. License Manager can display foreign keys but cannot deploy them.
- No keys selected. The keys previously selected are no longer present. This error is highly unlikely.
- Key string is invalid. The key selected is invalid. This error is highly unlikely because it implies a key previously validated has been corrupted.
- Problem deploying licensing information to this system. The system might be offline such as powered down or disconnected from the network. If not, an unusual unknown event occurred.

Related Topics

- License Manager
- Selecting Keys
- Collecting Keys

Managing Keys

The Manage Keys feature enables you to manage license keys from selected servers and Integrated Lights-Out (iLO) management processors. The keys managed include ProLiant Essentials keys for iLO and ProLiant Essentials products as well as selected products operating with foreign licensing schemes. The key or key facsimile can originate from direct user input and collect key process under user control or from automatic processes that include discovery and identification (for iLO only) and other automatic means.

The **Manage Keys** page provides you with a complete list of keys contained within the ProLiant Essentials licensing key database in table format on entry. On selecting a particular key, Manage Keys provides specific information on the use of that key.

To access the **Manage Keys** page, select **Deploy->License Manager->Manage Keys**. The **Manage keys** window appears.

You have the following options:

- “Viewing Key Details”. Select a key from the summary table to review details on its use.
- “Adding Key Individually”. Enter an individual key, view key details, and add the key to the database.
- “Adding Keys From a File”. Select a specially formatted key file, view key file contents, and add the keys to the database.

Related Topics

- License Manager
- Adding Keys From a File
- Adding Key Individually
- Viewing Key Details
- Collecting Keys
- Deploying Keys

Viewing Key Database Contents

HP Systems Insight Manager (HP SIM) enables you to view contents of the ProLiant Essentials licensing key database.

To view contents of the ProLiant Essentials licensing key database, access the Manage Keys page. Select **Deploy->License Manager->Manage Keys**.

The **Manage Keys** page displays all of the keys known to License Manager. You can double-click the appropriate column header to sort the list based on the entries in that column. The following columns display:

- **Product**. The name of the licensed product.
- **Version**. The version of the software for which the license is valid (higher versions support lower versions, but lower versions do not support higher versions). For example, a version 2 key would allow the version 1 products to run. A key valid to operate version 1 of the product would not grant permission to run the version 2 software product).
- **License Type**. Six types of licenses are available (refer to “About Keys” for more information).
- **Seats Max**. The total number of licenses permitted by the key.
- **Seats Used**. The number of licenses that are currently in use.
- **Days Max**. The total number of days authorized for use by this key (time specific keys only). For BETA key type, this is the number of days from the date the key was issued. For all others, it is the number of days from when the key was first used.
- **Key string**. The license key string

Related Topics

- License Manager
- Adding Keys From a File
- Viewing Key Details
- Collecting Keys
- Deploying Keys

Adding Keys From a File

HP Systems Insight Manager (HP SIM) enables you to add one or more keys to the database. The keys are defined in an XML file with a key extension. You can create these files if needed. The format is of the form:

```
<?xml version="1.0" encoding="UTF-8"?>
<KEYLIST>
<KEY>
<KEYSTRING>A2345-1B345-12C45-123D5-123E5</KEYSTRING>
<PRODUCTNAME1>SMP</PRODUCTNAME1>
<PRODUCTVERSION1>v1.0</PRODUCTVERSION1>
<KEYDISP1>3</KEYDISP1>
</KEY>
</KEYLIST>
```

For user created files, the minimal format is:

```
<?xml version="1.0" encoding="UTF-8"?>
<KEYLIST>
<KEY>
<KEYSTRING>A2345-1B345-12C45-123D5-123E5</KEYSTRING>
</KEY>
</KEYLIST>
```

With the key tag sequence repeated for each key to encode in the file.

To add one or more new keys to the database from a specially formatted key file:

1. Access the **Manage Keys** page, and select **Deploy>License Manager>Manage Keys**.
2. Click **Add Key from File**.

The **Add Key from File** section appears at the bottom of the page.

3. Enter the full path and file name in the **Specify a file name and path** field.
or
Click **Browse**.
 - a. The **Choose file** dialog box appears.
 - b. Navigate to the key file that contains the key codes to be added.
 - c. When a file has been located, click **Open**.
4. When the full path and file name display in the **Specify a file name and path** field, click **Open** to open the file. The contents of the key file are displayed.
5. Click **Add Keys** to add all the keys to the database. If for some reason a key is invalid, an error for that key is reported and that key is not added to the database.

Related Topics

- License Manager
- Adding Key Individually
- Collecting Keys
- Deploying Keys

Adding Key Individually

HP Systems Insight Manager (HP SIM) enables you to add individual keys to the database.

To add a key to the database individually:

1. Select **Deploy->License Manager->Manage Keys**.
2. Click **Add Key**.

The **Add a New Key** page appears.

3. Enter the key by entering it into the five fields as individual characters (five per field). The cursor automatically advances to the next field when the current field is full as you enter the key code starting from the left-most box.

or

Enter the key by pasting the entire key into and of the five input fields, for example, if you received a key as text in an e-mail.

4. Highlight the complete key string, and press the **Ctrl + C** keys to copy it.
5. Position the cursor in any of the five fields forming the input box, and press the **Ctrl + V** keys to paste the license key. You can also right-click to paste.

The license key displays with five characters in each of the five fields.

Note: When pasting in the complete key, the key can be in the normal format of five groups of five characters, with each separated by a hyphen (-), for example,

#####-#####-#####-#####-#####. There are no spaces between the field characters and the hyphens.

6. Click **Open** to display key details.
7. Click **Add Key** to add the new key to the database. An error message appears if the key is invalid and that key is not added to the database.

Related Topics

- License Manager
- Adding Keys From a File
- Collecting Keys
- Deploying Keys

Viewing Key Details

HP Systems Insight Manager (HP SIM) enables you to view license details for a specific key. Access the **Manage Keys** page. Select **Deploy->License Manager->Manage Keys**.

To view details on the use of a specific key, select the desired key:

- **System Name.** The name of the system that includes an instance of this key. The key might not be in use.
- **System Type.** The HP SIM defined system type of the named server, for example, server.
- **Seats Used.** The total number of seats in use that are linked to the selected key.
- **Days Max.** The total number of days authorized for use by this key (time-specific keys only). For BETA key type, this is the number of days from the date the key was issued. For all others, it is the number of days from when the key was first used.
- **Status.** The status of the use of this key on the named system.

Status messages include:

- OK. The key is valid and in compliance.
- Key not in use. The key is valid but not used.
- License is fully subscribed. The license key is in full use on this target and consequently, if used elsewhere as well, might be over subscribed in total.
- License is over subscribed. The license key is over used on this target.
- License trial period has expired. The time limit on a time limited key has been exceeded (for time limited keys).
- License time period has expired. The time limit on a time limited key has been exceeded (for time limited keys).
- License subscription period has expired. The subscription key has expired.
- Invalid license certificate. The key information as stored on this target system is invalid.

- Wrong host equipment. The serial number of the target on which this key was found does not agree with the serial number contained within the key information retrieved from this machine.

Related Topics

- License Manager
- Adding Keys From a File
- Collecting Keys
- Deploying Keys

System License Information Reporting

The System License Information Reporting feature provides a quick and efficient way to track ProLiant Essentials License Information for Integrated Lights-Out (iLO) systems. This reporting function also reports on the use of other ProLiant Essentials products based on license keys.

The iLO product must be configured to respond to license requests. This configuration page can be reached by selecting the appropriate **System Page**, clicking **Tools & Links**, and then clicking the link directed at the iLO. On the iLO, select **Administration>SNMP>Insight Manager Settings**. In the lower part of the page, locate the **Configure Insight Manager Integration** section. **The Level of Data Returned** must be set to **Enabled** or **Disabled**. If **The Level of Data Returned** is set to **Disabled**, the system is reported. However, the licensing state cannot be determined and the status indicates this with a message of `Not Available`. If **The Level of Data Returned** is set to **Disabled**, there is no license record.

If an iLO system is deleted from the management server database, the iLO licensing information saved for that system is deleted at the same time. For all other system types, such as servers, desktops, and the like, licensing information is never deleted.

In the reports for iLO, the **Product Version** field might be left blank. The **License Key** field might be blank even when that iLO does have a valid license (this occurs when the **Level of Data Returned** is set to **Disabled**). The iLO product is licensed if the **License Type** field is not blank. The **Number of Licenses in Use** field is the total usage of that license key on that particular system. With ProLiant Essentials licensing, a particular key can permit many concurrent uses of the licensed item. The **Number of Licenses in Use** reflects the use of that key on that system.

Note:



Run discovery to retrieve license information from iLO systems before running the **System License Information** report, or expect to see keys for iLO in the **License Manager - Manage Keys** summary table. Refer to “Configuring Automatic Discovery” for more information.

Note:



For the iLO product, the **Product Version** is left blank.

Reported license information is also collected from License Manager for all systems known to HP Systems Insight Manager (HP SIM) and from which License Manager has collected keys.

Only a user with full-configuration-rights has access to the license key. When running a report, this column is not shown to a user with limited or no configuration rights. When creating a report configuration, users with limited or no configuration rights cannot see or choose the **License Key** column.

System License Information Reporting

The **System License Information** report provides a summary on the details and distribution of licenses.

- System Name
- License Key
- Number of Licenses Purchased
- Number of Licenses in Use
- Key Version
- Product Name
- Product Version
- License Type
- License Date
- License Expiration Date (DEMO key only)
- Status

Refer to “Reporting Views”, R_DeviceLicenseInfo, for specific field information.

Upgrade Results

During upgrade, all report configurations are examined, and the iLO Licensing report items in those report configurations are mapped to the new **System License Information** report items. If the iLO report item of License Key is found in a report configuration in the old database, that report configuration is copied over to the new database, and the report configuration now refers to the new License Key. At the same time, the report items **Number of Licenses Purchased** and **Product Name** are inserted into the copied report configuration.

Related Procedure

- System Reporting
- Collecting Keys
- Deploying Keys
- Managing Keys

Related Topics

- Reporting
- Reporting Views
- System Reporting

Licensing with ProLiant Essentials Applications

The **License unlicensed systems (optional)** page appears when some of the targets selected are not licensed to use this product. Only those targets which are not licensed or licensed with a demo key are displayed.

This page is not directly accessible from the menus. It occurs in a sequence of one or more pages specific to a particular product. The same page is shared by all products using this page, so the page format and operation is the same for all products.

Four buttons are available from this page:

Previous. Click **Previous** to return to a previous page.

Add Key. If you have additional licenses available which are not yet known to HP Systems Insight Manager (HP SIM), you can add these keys. If you have a key string, click **Add Key** and enter the key in the **Specify a key string** field and click **OK**. Only license keys applicable to this product are accepted and added. To add other product keys, use License Manager, Manage Keys (**Deploy->License Manager->Manage Keys**).

Apply License. If there are licenses available for use, select the unlicensed targets you want to license and click **Apply License**. Targets licensed during some form of time limited demo key are also shown. These can be selected but can only be relicensed using a PAID key. After all targets are licensed, this page is not displayed again (in this sequence). If there are targets that are still not licensed or licensed with a demo key, this page redisplay showing the original list of unlicensed targets, indicating which target systems are now licensed and which are not. Selecting to license a target which has been licensed using a demo key will re-license the target with a permanent key, if a key is available. If there are insufficient licenses remaining at the time of the re-license, the demo license remains in force. When licensing, the full licenses (including those included with the product) are used first. If there are systems which remain unlicensed after all these licenses are consumed, any demo key not used to capacity is used if the product permits it. Finally, as other users might be attempting to license other targets for use with the product at the same time, it is possible to select a number of targets equal to the available licenses and yet fail to license some of those targets. A message advises when this has occurred.

Next. If you do not want to license any of these unlicensed targets or at any time after licensing some of those targets, you can continue directly by clicking **Next** provided at least one of the selected targets is licensed. If no selected targets are licensed, the **Next** button is displayed.

Upon successful completion, the number of licenses available should increase by the number of licenses enabled by the key. Those additional licenses are now available for use.

Note:



When some or all of the selected targets are licensed using a demo key, those targets appear in the not licensed table with a status of Licensed using a demo key. You can select any of these targets and re-license with a full key at this time. Demo and evaluation keys are not accepted to relicense a system with such a key.

Related Topics

- License Manager
- About Keys

Management Processor Tools

HP's Management Processor enables remote server management over the Web regardless of the system state. In the unlikely event that the operating system is not running, Management Processor can be accessed to power cycle the server, view event logs and status logs, enable console redirection, and more.

New menu items are displayed in HP Systems Insight Manager (HP SIM) after management processors are discovered.

- **System Power.** This tool enables you to control the power options on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems. To access, select **Tools>Management Processor>HP Integrity and HP 9000 iLO>System Power.**
- **System Locator.** This tool enables you to control the locator LED on one or more HP Integrity and HP 9000 iLO systems. To access, select **Tools>Management Processor>HP Integrity and HP 9000 iLO>System Locator.**
- **New User.** This tool enables you to add a new user account to one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure>Management Processor>HP Integrity and HP 9000 iLO>New User.**
- **Modify User.** This tool enables you to modify an existing user account on one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure>Management Processor>HP Integrity and HP 9000 iLO>Modify User.**
- **Delete User.** This tool enables you to remove an existing user account from one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure>Management Processor>HP Integrity and HP 9000 iLO>Delete User.**
- **LAN Access.** This tool enables you to modify LAN access settings on one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure>Management Processor>HP Integrity and HP 9000 iLO>LAN Access.**
- **LDAP Settings.** This tool enables you to configure the LDAP service on one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure>Management Processor>HP Integrity and HP 9000 iLO>LDAP Settings.**

- **iLO Control.** This tool enables you to execute internal control actions on one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure->Management Processor->HP Integrity and HP 9000 iLO->iLO Control**.
- **Firmware Upgrade.** This tool enables you to initiate a firmware upgrade through FTP on one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure->Management Processor->HP Integrity and HP 9000 iLO->Firmware Upgrade**.
- **Deploy SSH Public Key.** This tool enables you to deploy the HP Systems Insight Manager (HP SIM) SSH public key on one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure->Management Processor->HP Integrity and HP 9000 iLO->Deploy SSH Public Key**.

Related Procedures

- Creating New Users on Management Processors
- Editing Management Processor Users
- Deleting Management Processor Users
- Configuring LAN Access on Management Processors
- Configuring LDAP Settings on Management Processors
- Executing Internal Control Actions through Management Processors
- Upgrading Management Processor Firmware
- Deploying SSH Public Keys to Management Processors

Controlling System Power Options through Management Processors

This tool enables you to control the power of one or more servers through the associated HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To set the system power control:

1. Select **Tools->Management Processor->HP Integrity and HP 9000 iLO->System Power**. The **System Power** page appears.
2. Select target systems and click **Next**. Refer to “Creating a Task” for information on selecting targets. The **Step 2: Select an action** page appears.
3. Under **System power control**, select one of the following:
 - Power cycle
 - Power on
 - Power off
 - Graceful shutdown (except HP9000)
4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule the task to run at another time, or click **Previous** to return to the previous **System Power** page. Refer to “Scheduling a Task” for more information on scheduling a task.

Related Procedure

- Controlling the System Locator LED through Management Processors

Controlling the System Locator LED through Management Processors

This tool enables you to control the locator LED on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To control the system locator:

1. Select **Tools->Management Processor->HP Integrity and HP 9000 iLO->System Locator**. The **System Locator** page appears.
2. Select target systems and click **Next**. Refer to “Creating a Task” for information on selecting targets. The **Step 2: Select an action** page appears.
3. Under **System locator/Unit Identification LED**, select one of the following:
 - On
 - Off
4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule the task to run at another time, or click **Previous** to return to the previous **System Power** page. Refer to “Scheduling a Task” for more information on scheduling a task.

Related Procedure

- Controlling System Power Options through Management Processors

Creating New Users on Management Processors

This tool enables you to add a new user account to one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To create a new user:

1. Select **Configure->Management Processor->HP Integrity and HP 9000 iLO->New User**. The **New User** page appears.
2. Select target management processors and click **Next**. Refer to “Creating a Task” for information on selecting targets. The **Step 2: Select an action** page appears.
3. Under **Enter properties for a new user account**, enter:
 - **Login id.** (Mandatory) This is the name that must be used when logging into iLO. The maximum length for a Login Id is 25 characters.
 - **Password.** (Mandatory) The password must be provided when logging into iLO. The password must be a minimum of 6 characters with a maximum of 24 characters.

- **Password (Verify).** (Mandatory) The password must be provided a second time for verification.
 - **User name.** (Mandatory) This name appears in the iLO user list. It is not necessarily the same as the login name. The maximum allowed length is 25 characters.
4. Under **Access Rights**, select the one or more access rights for the user. Usually, a new user is granted the Console Access right.
 - **Console access**
 - **Power access**
 - **Management processor configuration**
 - **User administration**
 5. Click **Run Now** to run the task immediately. Click **Previous** to return to the previous **New User** page.

Related Procedures

- Controlling the System Locator LED through Management Processors

Editing Management Processor Users

This tool enables you to modify an existing user account on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To modify a user:

1. Select **Configure>Management Processor>HP Integrity and HP 9000 iLO>Modify User**. The **Modify User** page appears.
2. Select target management processors and click **Next**. Refer to “Creating a Task” for information on selecting targets. The **Step 2: Enter properties to modify an existing user account** page appears.
3. Under **Enter the login name of the user account you wish to modify**, enter the **Login id** to be modified.
4. Under **Select the properties you wish to modify for this user account:**, select the attribute to modify and enter the appropriate information. Select from:
 - **Password.** If you select to change the password, verify the password in the **Password (Verify)** field.
 - **User name.** Select this field to modify the user name. This is not necessarily the same as the login name. The maximum allowed length is 25 characters.
 - **Access rights.** If you select to modify the access rights, select from **Console access**, **Power access**, **Management processor configuration**, and **User administration**. To remove all access rights for an account, select the **Access rights** checkbox and leave the

Consol access, Power access, Management processor configuration, and User administration checkboxes deselected.

- Click **Run Now** to run the task immediately. Click **Previous** to return to the previous **Modify User** page.

Related Procedures

- Creating New Users on Management Processors
- Deleting Management Processor Users

Deleting Management Processor Users

This tool enables you to remove an existing user account from one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To delete a user:

- Select **Configure>Management Processor>HP Integrity and HP 9000 iLO>Delete User**. The **Delete User** page appears.
- Select target management processors and click **Next**. Refer to “Creating a Task” for information on selecting targets. The **Step 2: Enter properties to delete an existing user account** page appears.
- Enter the **Login id** to be deleted.
- Click **Run Now** to run the task immediately. Click **Previous** to return to the previous **Delete User** page.

Note:

HP Systems Insight Manager (HP SIM) uses the Admin account to execute Management Processor tools. If this account is removed from the iLOs, the tools will not be able to access the iLOs on those systems, unless tool execution is reconfigured.

To configure HP SIM tool execution on a different iLO account:



- Select a user account that is to be used to run tools on iLOs. This user account must be present on all managed iLOs and must have all rights on the iLOs.
- Navigate to the tools directory on the central management server (CMS) and edit `MpTools.xml`.
- Find each `<execute-as-user>` line in the XML file and change `Admin` to the user account specified in step 1.
- Run `mxtool -m -f MpTools.xml -x force`.
- On the CMS, run `mxagentconfig` or the Deploy SSH Public Key tool to copy the authentication keys for this user account to each managed iLO. Refer to

“Deploying SSH Public Keys to Management Processors” for more information on deploying the SSH public key.

Related Procedures

- Creating New Users on Management Processors
- Editing Management Processor Users

Configuring LAN Access on Management Processors

This tool enables you to modify LAN access settings on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To modify LAN access:

1. Select **Configure>Management Processor>HP Integrity and HP 9000 iLO>LAN Access**. The **LAN Access** page appears.
2. Select target management processors and click **Next**. Refer to “Creating a Task” for information on selecting targets. The **Step 2: Enter LAN access settings** page appears.
3. Under **Select the settings you wish to configure and choose their values**, select from:
 - **Telnet access.** Select to **Enable** or **Disable** Telnet access. This does not affect the IP configuration or the ability of the management processor to perform upgrades over the LAN.
 - **Web SSL.** Select to **Enable** or **Disable** Web SSL.
 - **Web console port.** If you select this option, you must enter a valid port number. Valid port numbers are 23 and 2000 through 2400.
 - **IPMI over LAN access.** Select to **Enable** or **Disable** IPMI over LAN access.
4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule when the task runs, or click **Previous** to return to the previous **LAN access** page. Refer to “Scheduling a Task” for information on scheduling a task.

Configuring LDAP Settings on Management Processors

This tool enables you to configure the LDAP service on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To configure the LDAP service:

1. Select **Configure>Management Processor>HP Integrity and HP 9000 iLO>LDAP Settings**. The **LDAP Settings** page appears.
2. Select target management processors and click **Next**. Refer to “Creating a Task” for information on selecting targets. The **Step 2: Enter LDAP directory settings** page appears.

3. Under **Select the settings you wish to configure and choose their values**, select from the following:
 - **Local user accounts.** Select to **Enable** or **Disable** access to local iLO user accounts. If local user accounts are enabled, a user can log into iLO using locally stored user credentials. If local user accounts are disabled, user access is limited to valid directory credentials only.
 - **Directory authentication.** Select to **Enable** or **Disable** to activate or deactivate directory support on the selected iLOs. If directory authentication is enabled and configured properly, users can log into iLO using directory credentials. If this is disabled, user credentials are not validated using the directory.
 - **Directory server IP address.** Enter the IP address of the directory server.
 - **Directory server LDAP port.** Enter the LDAP for secure LDAP service on the server. The default value for this port is 636.
 - **Distinguished name.** Specifies where this iLO instance is listed in the directory tree. For example: *cn=MP Server.ou=Management Devices.o=hp*
 - **User search context 1.** User name contexts that are applied to the login name entered to access iLO.
 - **User search context 2.** User name contexts that are applied to the login name entered to access iLO.
 - **User search context 3.** User name contexts that are applied to the login name entered to access iLO.
4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule when the task runs, or click **Previous** to return to the previous **LDAP Settings** page. Refer to “Scheduling a Task” for more information on scheduling a task.

Executing Internal Control Actions through Management Processors

This tool enables you to execute internal control actions on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To execute internal control actions:

1. Select **Configure>Management Processor>HP Integrity and HP 9000 iLO>iLO Control**. The **iLO Control** page appears.
2. Select target management processors and click **Next**. Refer to “Creating a Task” for information on selecting targets. The **Step 2: Select one or more actions** page appears.
3. Select one or both of the options listed:
 - **Clear event logs.** This option clears the system event logs.
 - **Reset management processor.** This option executes a reset of the iLO.

4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule when the task runs, or click **Previous** to return to the previous **iLO Control** page. Refer to “Scheduling a Task” for more information on scheduling a task.

Upgrading Management Processor Firmware

This tool enables you to initiate a firmware upgrade through FTP on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems. The upgrade is performed simultaneously on all selected iLOs.

To initiate a firmware upgrade:

1. Select **Configure>Management Processor>HP Integrity and HP 9000 iLO>Firmware Upgrade**. The **Firmware Upgrade** page appears.
2. Select target management processors and click **Next**. Refer to “Creating a Task” for information on selecting targets. The **Step 2: Specify firmware upgrade parameters** page appears.
3. Enter the following information:
 - **Source IP.** The user must enter the IP address of the ftp server.
 - **File path.** The path to the directory (on the ftp server) in which the upgrade files reside.
 - **Login ID.** The login ID used to log into the ftp server.
 - **Password.** The password to the ftp server.
4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule when the task runs or click **Previous** to return to the previous **Firmware Upgrade** page. Refer to “Scheduling a Task” for more information on scheduling a task.

Deploying SSH Public Keys to Management Processors

This tool enables you to deploy the HP Systems Insight Manager (HP SIM) SSH public key on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems. Prior to executing this tool, SSH must be enabled on the target iLO and SSH keys must have been generated on the iLO. This tool must be executed once after initial installation or after the central management server (CMS) public key has changed. It is a prerequisite to executing any of the Management Processor tools.

This tool must be run from an account that has administrative privileges on the HP SIM CMS.

To deploy the HP SIM SSH public key:

1. Select **Configure>Management Processor>HP Integrity and HP 9000 iLO>Deploy SSH Public Key**. The **Deploy SSH Public Key** page appears.
2. Select target management processors and click **Next**. Refer to “Creating a Task” for information on selecting targets. The **Step 2: Enter login credentials** page appears.
3. Enter credentials for the administrator account on the target iLOs.

- **User name.** This is an administrative account on the managed iLO. Usually it is the Admin account.
 - **Password.** This is the administrative account password on the managed iLOs.
 - **Password (Verify).** Verify the password.
4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule when the task runs, or click **Previous** to return to the previous **Deploy SSH Public Key** page. Refer to “Scheduling a Task” for more information on scheduling a task.

Managing MIBs

A Management Information Base (MIB) is a file that contains information that enables you to correctly interpret specific information from systems on your network and gives you a more precise view of the activity on your network. To take advantage of this capability, the MIB must be registered to HP Systems Insight Manager (HP SIM). Refer to “Registering a MIB” for more information.

HP has defined MIBs for its systems, and these MIBs expose the rich management infrastructure that HP builds into its products. HP MIBs are already registered in the HP SIM database. You can find them in the directory `\hp\system insight manager\mibs` on a Windows CMS or `opt\mx\mibs` on a UNIX CMS. If you have third-party systems on your network, you can register the MIBs that accompany the systems. Refer to “Registering a MIB” for more information regarding registering your MIBs. Registering allows the MIBs to be identified correctly and traps can be interpreted correctly to give you a more precise view of the activity on your network. Always register the most recent version of a third-party MIB.

Related Procedures

- Registering a MIB
- Unregistering a MIB
- Compiling a MIB
- Editing a MIB

Viewing a MIB

After a Management Information Base (MIB) has been registered in the HP Systems Insight Manager (HP SIM) database, additional `mxmib` options, such as `mxmib -l` and `mxmib -t` can be used to view all MIBs added to the database and all traps associated with a particular MIB. Also, SNMP Trap Settings (**Options->Events->SNMP Trap Settings**) can be used to display all registered MIBs and their associated traps that are contained in the database. The Event Type, Description, Enable Trap Handling, Category, and Severity can be modified through this screen to further customize the information that is collected on the network. Refer to “Editing a MIB” for more information regarding editing a MIB.

Warning!



Do not rename, move, or delete MIB files from the directory after they are registered.

Note:



For a MIB file to be listed as registered, the MIB file must reside in the MIBs directory.

Note:



The following HP SIM directories are default directories. However, the directories can vary depending on the directory specified during HP SIM installation.

To view a MIB on a Windows operating system:

1. Navigate to the MIB directory at `c:/program files/hp/systems insight manager/mibs`.
2. Open the MIB with an ASCII editor.
3. Enter **write cpqghost.mib** on the Windows command line.

To view a MIB on a Linux or HP-UX operating system:

1. Enter **cd opt/mx/mibs**.
2. Run **mxmib -l** to view registered MIBs.
3. Enter **vi file.mib** from a shell prompt.

Related Procedures

- Registering a MIB
- Unregistering a MIB
- Compiling a MIB
- Editing a MIB
- Configuring SNMP Traps

Related Topic

- Managing MIBs

Editing a MIB

The HP MIBs configuration (`.cfg`) file can be edited with trap specific information, such as:

- *TYPE*. The type is a simplified form of the actual trap name. Change the type if it does not adequately describe the device for you.

- *SEVERITY*. Some vendors use the default `INFORMATIONAL` for all severity levels. Change the severity to a level that reflects your judgment of the problem. Alternatively, you can change a Major or Critical severity for a trap message that is clearly not a critical situation in your environment. Only you know if this is the case. The only valid options for HP Systems Insight Manager (HP SIM) are: `Critical`, `Major`, `Minor`, `Warning`, and `Informational`.
- *MSG_FORMATTER*. This is a message formatting string used to construct enhanced messages that might be sent to a pager or in an e-mail. This string can be modified in the REV or the MIB.
- *ENABLE*. By default all traps are enabled. Trap handling gives you control over the volume of messages. Shut off nuisance messages, such as unnecessary informational messages or repeated trap messages, for an event that has not been corrected.
- *DESCRIPTION*. The description is vendor-supplied. Replace it with more specific instructions, a precise reference source, or a website referral.
- *CATEGORY*. The category lists the HP SIM category types and `UNKNOWN`.

To edit the `.cfg` file:

1. Navigate to the MIB directory:
 - For Windows operating systems, navigate to `\program files\hp\systems insight manager\mibs`.
 - For Linux or HP-UX operating systems, navigate to `/opt/mx/mibs`.
2. Run `mcompile mymib.mib` to create the `.cfg` file.
3. After the `.cfg` file is created, use an editor of your choice to edit the `.cfg` file.

To edit trap-specific information in HP SIM:

1. From HP SIM, select **Options->Events->SNMP Trap Settings**.
The **SNMP Trap Settings** page appears.
2. Select the MIB name.
3. Select the trap within the MIB to be edited.
4. Edit the file with your changes, and click **OK** to save your changes.

Note: The changes made through the **SNMP Trap Settings** page are saved to the HP SIM database only. The `.cfg` and MIB files are not affected.

Related Procedures

- Viewing a MIB
- Compiling a MIB
- Unregistering a MIB

Related Topic

- Managing MIBs

Compiling a MIB

The **mcompile** command enables you to compile an SNMP MIB file into an intermediate format (`.cfg`) file that can be registered using the **mxmib** utility for use with HP Systems Insight Manager (HP SIM).

Observe the following tips:

- If the MIB file being compiled includes **IMPORTS** from other MIBs, the imported MIB files should also be located in the same directory as the MIB file being compiled.
- Comment lines in MIB files start with "--" and end with a new line or the next occurrence of "--". Beware of MIBs with "--" characters across the entire line. These lines are intended to be comments. However, extra dashes have canceled the first set of "--" characters.

For example:

```
-- xyz comments out xyz.
```

However:

```
-- -- xyz effectively uncomments xyz.
```

- **mcompile** expects the *END* keyword at the end of a module on a line by itself. Be sure there is a new line in the MIB file after the *END* keyword.
- **mcompile** does not allow redefinition of standard data types. If the MIB file being compiled contains such redefinitions, they should be commented out before running **mcompile**.

To compile a MIB:

1. Open an MS-DOS® window or UNIX shell.
2. Run **mcompile** to compile an SNMP MIB file into an intermediate format (`.cfg`).

mcompile recognizes the `-d` option. This option changes to the specified directory to locate and process the MIB file. The intermediate (`.cfg`) file is always placed in the same directory as the MIB file. By default, **mcompile** searches for the MIB file in the current directory.

For example:

```
cd mibsdir
```

```
mcompile mymib.mib
```

or

if you are not running in the MIBs directory:

```
mcompile -d mibsdir mymib.mib
```

3. Run **mxmib** to register the MIB with HP SIM.

Related Procedures

- Registering a MIB

- Unregistering a MIB
- Viewing a MIB
- Editing a MIB

Related Topic

- Managing MIBs

Registering a MIB

HP Systems Insight Manager (HP SIM) ships with HP MIBs that are registered at installation. In addition, a number of pre-compiled MIBs are included in the form of `.cfg` files. These MIBs can be registered at your convenience. A number of those `.cfg` files have been edited. If the corresponding MIB is recompiled, then those edits are lost.

To view a list of currently registered MIBs, including MIBs that you have registered:

- In Windows, enter `dir "c:\program files\hp\systems insight manager\MIBs*.MIB"` at the command line.
- On UNIX, enter `ls /opt/mx/mibs/*.mib` at the command line.

To view MIBs that are preloaded and registered during HP SIM installation:

- In Windows, enter `type "c:\program files\hp\systems insight manager\MIBs\cfglist?.list"` at the command line.
- On UNIX, enter `cat /opt/mx/mibs/cfglist*.list` at the command line.

Note:



These are the install directories. If you changed the install directory during the HP SIM installation, these commands must reference your path instead.

HP MIBs can be registered using the command line interface (CLI). The CLI is the same for all CMS types including Windows, Linux, and HP-UX.

Note:



When registering a MIB, it is not always necessary to run `mcompile` on the MIB especially if the corresponding `.cfg` file to that MIB already exists. If you run `mcompile` on a MIB and a `.cfg` file exists, a new `.cfg` is generated, which supersedes the old `.cfg` file and any changes in the old file will not be active. In most cases with an existing `.cfg` file, it is desirable to edit the `.cfg` file to make changes unless a new MIB has been furnished.

This `.cfg` file can then be registered to the HP SIM database using the `mxmib -a` or `mxmib -f` command.

To register a MIB in HP SIM:

1. Open an MS-DOS window or UNIX shell.
2. Use an editor of your choice to create a file containing a list of the `.cfg` files to be registered. One `.cfg` per line.
3. Run `mxmib -f cfglist.list` to import a list of MIBs into HP SIM. After the MIB is registered in HP SIM, you can use `mxmib` to list or delete the MIB from HP SIM.

Note: You can also use `mxmib -a mymib.cfg` to register a single MIB.

Note: The `.cfg` file being registered must be in the MIBs directory.

Related Procedures

- Viewing a MIB
- Compiling a MIB
- Unregistering a MIB
- Editing a MIB

Related Topics

- Managing MIBs
- Service Notification Events

Unregistering a MIB

HP MIBs can be unregistered using the command line. The command line interface (CLI) is the same for all CMS types to include Windows, Linux, and HP-UX.

To unregister a MIB from HP SIM:

1. Open an MS-DOS window or UNIX shell.
2. Run `mxmib -d file.mib` to unregister the MIB in HP Systems Insight Manager (HP SIM).

Related Procedures

- Viewing a MIB
- Compiling a MIB
- Registering a MIB
- Editing a MIB

Related Topics

- Managing MIBs
- Service Notification Events

Installing OpenSSH

HP Systems Insight Manager (HP SIM) custom commands and command line tools require that Secure Shell (SSH) be installed and configured on each of the managed systems to work properly.

Refer to Secure Shell (SSH) in HP Systems Insight Manager white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more detailed information on SSH and the features in HP SIM that use SSH.

The OpenSSH install is run from the central management server (CMS) and installs the OpenSSH service onto target Windows systems and then runs the **mxagentconfig** command to complete the configuration.

Note:



To be sure that the install OpenSSH task runs successfully, you should be signed in as Administrator. If you are logged on as another user, be sure the user name does not contain any non-ASCII characters.

To install OpenSSH through the OpenSSH Install option:

1. Select **Deploy->Deploy Drivers, Firmware and Agents->Install OpenSSH**. The **Install OpenSSH** page appears.
2. Select the target systems. Refer to “Creating a Task” for more information on selecting target systems.
3. Click **Next**.
4. From the **Enter credentials for an administrator account on the target system(s)**: section:
 - a. In the **User name** field, enter the Windows administrator user name.
 - b. In the **Password** field, enter the administrator password for the Windows user name entered in the previous step.
 - c. In the **Password (Verify)** field, re-enter the Windows administrator password exactly as it was entered in the **Password** field.
 - d. In the **Domain** field, enter the Windows domain.

Note: Leave **Domain** field blank if the administrator account on the target systems is a local account.
5. Click **Schedule** to schedule the install, or click **Run Now** to run the installation immediately. Refer to “Scheduling a Task” for more information on scheduling the installation.

If you clicked **Run Now**, the **Tasks Results** page appears. Refer to “Viewing Task Results” for more information on the **Task Results** page.

Related Procedures

- Creating a Task
- Scheduling a Task
- Viewing Task Results
- Initial ProLiant Support Pack Install
- Deploying OpenSSH to Multiple Systems Using RDP

- Creating an OpenSSH Task Through the CLI

Deploying OpenSSH to Multiple Systems Using RDP

OpenSSH can be installed on a target server using Rapid Deployment Pack (RDP), and then the HP Systems Insight Manager (HP SIM) public key can be copied to target systems.

Installing OpenSSH Using RDP

1. Copy the OpenSSH install component to the Deployment Server.
2. Create a new job.
3. Add a Copy File task by selecting **Add >> Copy File to**.
4. Ensure that the **Copy File** radio button is selected.
5. For the **Source path:**, enter the complete path where the OpenSSH installer is located. For example, if `OpenSSH_3.7.1p1-1.exe` is in folder `C:\temp\OpenSSH`, enter the source path as `C:\temp\OpenSSH\OpenSSH_3.7.1p1-1.exe`.
6. Under **Destination path:**, enter the location where you want this file to be copied on the target server. For example, if you want the file to be copied to the `C:\temp\OpenSSH` folder on the target server, enter the destination path as `C:\temp\OpenSSH\OpenSSH_3.7.1p1-1.exe`.
7. Click **Finish**.
8. Add a Run Script task to the job by clicking **Add >> Run Script**.
9. Ensure that the **Run this script** radio button is selected.
10. In the box below **Run this script**, enter the following:

```
C:\temp\OpenSSH\OpenSSH_3.7.1p1-1.exe /SILENT /NORESTART
```
11. Select the Windows radio button in the **In which OS would you like to run this script?** section.
12. Click **Finish**.
13. Drag this event and drop it on any system on which you want OpenSSH installed.

Copying the public key from HP SIM to the Target Systems

After OpenSSH is installed, create another script to copy the `dtfsshkey.pub` file (the public key) from the HP SIM server to the `.ssh` directory of the home directory of the administrator user on the target system.

1. Copy the `.dtfSshKey.pub` file from `..\Program Files\HP\System Insight Manager\config\sshtools\` folder on the HP SIM server to a local folder on the deployment server, and rename `.dtfSshKey.pub` to `authorized_keys2`.
 - a. Create a new job.

- b. Add a Run Script task to the job by clicking **Add >> Run Script**.
- c. Ensure that the **Run this script** radio button is selected.
- d. In the box below **Run this script**, enter the following (assuming that administrator's home directory is C:\Documents and Settings\Administrator):

```
cd C:\Documents and Settings\Administrator\
```

```
mkdir .ssh
```

```
cd .ssh
```

```
del * /q
```

- e. Select the Windows radio button in the **In which OS would you like to run this script?** section.
- f. Enter the complete path where you have the `authorized_keys2` file as the **Source path**: For example, if `authorized_keys2` is in folder C:\temp\OpenSSH, enter source path as C:\temp\OpenSSH\authorized_keys2.
- g. Enter the location where you want this file to be copied on the target server under the **Destination path**: For example, if the administrator's home directory is C:\Documents and Settings\Administrator, enter the destination path as C:\Documents and Settings\Administrator\.ssh\authorized_keys2.
- h. Click **Finish**.
- i. Add a Run Script task to the job by clicking **Add >> Run Script**.
- j. Ensure that the **Run this script** radio button is selected.
- k. In the box below **Run this script**, enter the following command:

```
net stop opensshd
```

```
net start opensshd
```

- l. Select the Windows radio button in the **In which OS would you like to run this script?** section.
- m. Click **Finish**.

2. Drag this event and drop it on the target system where you want OpenSSH to be configured.

Related Procedures

- Installing OpenSSH
- Initial ProLiant Support Pack Install
- Creating an OpenSSH Task Through the CLI

Creating an OpenSSH Task Through the CLI

Perform this procedure to create an OpenSSH task through the command line using the `mxtask` command in two ways:

- Entering all parameters through the command line
- Entering all parameters through an XML file

Note:



Tasks created from an XML file are disabled when viewed in the task list. Tasks created from the command line are not disabled when viewed from the task list.

Creating an OpenSSH Task

1. To see how to enter the information correctly, export an existing OpenSSH task.
 - a. Create an OpenSSH task. Refer to "Installing OpenSSH" for more information.
 - b. Save the task as **SSH Task**.
2. From the command line, execute the following command:

```
mxtask -lf "SSH Task" > ssh.xml
```

The `ssh.xml` now contains the format required to create an OpenSSH task from the command line. The following is an example file.

```
<?xml version="1.0" encoding="windows-1252"?>
<task-list>
  <task name="Install OpenSSH 1" type="manual"
    owner="admin" state="enabled">
    <toolname>Install OpenSSH</toolname>
    <queryname></queryname>
    <scheduleinfo />
    <timefilter />
    <toolparams>
      <?xml version="1.0"?>
      <XObject
        className="com.hp.mx.portal.taskandjob.
```

```
OpenSSHInstall.MxOpenSSHInstallCommandToolParameters"
classVersion="1.0">
  <Property name="driveLetter">
    <Simple>C:</Simple>
  </Property>
  <Property name="path">
    <Simple>C:\Program Files\HP\System Insight Manager\
      openssh\1118786323238</Simple>
  </Property>
  <Property name="component">
    <Simple>CP005309.EXE</Simple>
  </Property>
  <Property name="username">
    <Simple>administrator</Simple>
  </Property>
  <Property name="password">
    <Simple></Simple>
  </Property>
  <Property name="domain">
    <Simple></Simple>
  </Property>
</XeObject>
</toolparams>
</task>
</task-list>>
```

The OpenSSH task uses six parameters, even though the user is only asked for three during the task creation from the GUI. The first three parameters must follow the example provided. For example:

- **driveLetter.** Must be the drive on which HP Systems Insight Manager (HP SIM) is installed.
- **path.** Must be *full path to openssh dir\dir name*.
where *dir name* is any name you select.
- **component.** Must be CP005309.EXE.
- **username.** Is a user account with administrative rights on the target systems.
- **password.** Is the password to the administrative account specified by 'username.'
- **domain.** Is the domain of the administrative user (leave this blank if the administrative user is a local account on the target systems).

Creating an OpenSSH Task from the Command Line With an XML File

Execute:

```
mxtask -cf ssh.xml
```

Creating an OpenSSH Task from the Command Line Without an XML File

Execute:

```
mxtask -c taskname -q queryname -w schedule -t  
toolname -A toolparams
```

where *taskname* is the name you are giving the task, *queryname* is the name of an existing collection, *schedule* is **Tmanual**, *toolname* is the tool (installing OpenSSH), and *toolparams* are those listed previously.

For example:

```
mxtask -c "ssh1" -q "All Systems" -w Tmanual -t "Install OpenSSH"  
-A "<?xml version="1.0"?>  
<XeObjectclassName="com.hp.mx.portal.taskandjob.  
OpenSSHInstall.MxOpenSSHInstallCommandToolParameters"  
classVersion="1.0">  
<Property name="driveLetter">  
<Simple>C:</Simple>  
</Property>  
<Property name="path">  
<Simple>C:\hpsim\target\windows\stage\sim\openssh\  
1079128853916</Simple>  
</Property>  
<Property name="component">  
<Simple>CP005309.EXE</Simple>  
</Property>  
</Property name="username">  
<Simple>user1</Simple>  
</Property>  
</Property name="password">  
<Simple>password</Simple>  
</Property>  
<Property name="domain">  
<Simple>openview</Simple>  
</Property>  
</XeObject">
```

Related Procedures

- Installing OpenSSH
- Deploying OpenSSH to Multiple Systems Using RDP

PMP Tools

HP ProLiant Essentials Performance Management Pack (PMP) is an integrated performance management solution that detects and analyzes hardware bottlenecks on HP ProLiant servers, select HP Integrity servers, and MSA500/MSA1000/MSA1500 shared storage systems. PMP is automatically installed with HP Systems Insight Manager (HP SIM) and operates in integration with HP SIM. No software installation on the monitored servers is required, other than the Insight Management Agents. PMP analyzes performance information to determine if there is a building or existing performance bottleneck issue. You can interactively display this information, log the information to a database for later analysis or reporting, and set up proactive notification using the HP SIM notification mechanism.

Two ideal environments for use of PMP are:

Customers that want to know about and deal with server performance issues before they impact user productivity.

- PMP provides a concise overview of configuration anomalies that could impact performance, like faster drives on slower controllers, Network Interface Cards (NICs) set to half-duplex, Peripheral Component Interconnect (PCI) cards concentrated on a single PCI bus, and so forth
- PMP provides early alerts of building performance bottleneck situations
- PMP enables interactive and historical analysis of performance issues
- PMP provides clear-cut recommendations for solving performance issues

Customers that, due to budget constraints, cannot automatically replace servers every three years.

- PMP provides detailed information on the subsystem that causes performance constraints, enabling pinpointed upgrades to economically extend the useful life of a server
- Once economical upgrade possibilities are exhausted, PMP provides a summary report containing both a performance profile (showing for each of the subsystems the percentage of time that performance is out of spec) and a detailed server inventory for each subsystem

There are two PMP tools available through HP SIM **Optimize** menu:

Note:



These options are only available on a Windows system and not on HP-UX or Linux.

- **Online Analysis.** Enables you to watch and analyze the real-time performance of a monitored server. It provides an intuitive interface to detail the performance status and inventory of monitored servers, processors, memory, storage, network connections, and host bus nodes for each server.

To access **Online Analysis**, select **Optimize>Performance Management Pack>Online Analysis**.

or

From the **All Systems** collection page, select the monitored server by clicking its icon in the **PF** column.

To access help for this option, go to https://middle_tier:2381/pmp/help/Server_Status.htm where *middle_tier* is the name or IP address of the server that HP SIM and PMP are installed, or access `PMP_directory\Program Files\HP\Performance Management Pack\htm\help\Server_Status.htm` where *PMP_directory* is the PMP directory on the server that PMP is installed.

- **Offline Analysis.** Enables you to view recorded data sessions directly from the PMP repository.

To access **Offline Analysis**, select **Optimize>Performance Management Pack>Offline Analysis**.

To access help for this option, go to https://middle_tier:2381/pmptools/help/Offline Analysis.htm where *middle_tier* is the name or IP address of the server that HP SIM and PMP are installed, or access `PMP_directory\Program Files\HP\Performance Management Pack\PMPTools\htm\help\Offline Analysis.htm` where *PMP_directory* is the PMP directory on the server that PMP is installed.

Go to

<http://h18013.www1.hp.com/products/servers/proliantessentials/valuepack/pmp/index.html> for more information on PMP and access to documentation.

Related Topics

- PMP Administrative Options
- PMP Reporting Options

Removing and Restoring Tools

Removing a Tool

The Remove a Tool tool, removes a tool from the menu for all users in HP Systems Insight Manager (HP SIM). The tool name must match the name in the tool definition file.

Warning!



This tool can remove any tool, including tools supplied by HP.

To remove a tool from HP SIM:

1. Select **Options->Remove a Tool**. The **Remove a Tool** page appears.
2. Under **Parameters**, add information using the standard tool parameters. **Tool name** is the only required field.
3. Click **Run Now** to run the task immediately or **Schedule** to schedule when the task runs. Refer to “Scheduling a Task” for more information on scheduling a task.

To remove tools using the command line, enter

```
mxtool -r -t badtool
```

where *badtool* is the name of the tool you want to delete. Refer to `mxtool(1M)` [`man/mxtool.1m.html`] for more information.

Restoring a Tool

To restore a tool using the command line, enter:

```
mxtool -a -f /home/user1/defs/mytooldef
```

where `/home/user1/defs/` is the folder of the user restoring the tool and *mytooldef* is the tool to be restored. Refer to `mxtool(1M)` [`man/mxtool.1m.html`] for more information.

Related Procedures

- New Command Line Tool
- New Copy a File Tool
- New Web Launch Tool
- New X Window Tool

Related Topics

- Command Line Tools
- Command Line Tools Reference

Replicate Agent Settings

Replicate Agent Settings is source system configuration that can, during task setup, be edited and copied to a target system or group of systems.

To access Replicate Agent Settings, select **Configure->Replicate Agent Settings**. To select target systems, refer to “Creating a Task” for more information. After you click **Next** the **Choose Source**

System page appears. Select the source system. Refer to “Creating a Replicate Agent Settings Task” for more information.

Related Procedure

- Creating a Replicate Agent Settings Task

Related Topics

- Replicate Agent Settings - Reference
- About Secure Task Execution
- Replicating Trusted Certificates

Creating a Replicate Agent Settings Task

The Replicate Agent Settings tool enables HP Systems Insight Manager (HP SIM) to retrieve and optionally edit Web Agent configuration settings from a source system and distribute that configuration remotely to one or more target systems through Web Agents.

To set up a Replicate Agent Settings task, pick a system on which to base the configuration (the source system).

To create a Replicate Agent Setting Task:

1. Select **Configure>Replicate Agent Settings**. The **Replicate Agent Settings** window appears.
2. Select target systems. Refer to “Creating a Task” for more information.
3. Click **Next**.
4. Select a source system by selecting one of the following two methods:
 - **You know the name of the system.** If you select this option, enter the name of the system in the box. Click **Next**.
 - **Pick the system from a list.** If you select this option, select a target system from the list of known systems that support Replicate Agent Settings. Click **Next**.

Note: If the source system cannot be used, a message appears, informing you of the error. Select a different system from the **Choose Source System** page.

Note: If the trust relationship for a system is incorrectly configured, an error message appears. Refer to “Replicate Agent Settings - Reference” for more information.

The **Choose Source Configuration Settings** page appears. The source system configurations display without any parameters selected.

5. Select the desired settings as needed. You can select each parameter individually. At least one must be selected to continue. You can also select to **Wake target systems from low power mode before configuring**. Refer to “Replicate Agent Settings - Reference” for more information.
6. Select one of the following options to execute the task:

- Click **Schedule** to schedule when the task should run. Refer to “Scheduling a Task” for more information.
- Click **Run Now** to run the task immediately. The **Task Results** page appears. Refer to “Task Results List” for more information.
- Click **Previous** to return to the previous page.

Note: The Replicate Agent Settings task uses the Secure Task Execution (STE) feature. Refer to “About Secure Task Execution” for more information.

Related Procedure

- Scheduling a Task

Related Topics

- Replicating Trusted Certificates
- Replicate Agent Settings - Reference
- About Secure Task Execution

Replicate Agent Settings - Reference

Determining the Trust Relationship

When picking the source system from the list, a trusted column displays that indicates whether a trust relationship exists between the management server and the indicated system. If a trust relationship is not configured for that system, that system is marked **no** in the trusted column.

Changing a Trust Relationship

To change a trust relationship for a system, click **configure** in the appropriate row. The HTTP server configuration page or **System Management Homepage** for the associated system appears.

Wake on LAN feature

Wake on LAN (WOL) is a feature that is used by HP Systems Insight Manager (HP SIM) to bring a target system that is in Advanced Configuration Power Interface (ACPI) Standby mode or powered off to full power. The Replicate Agent Settings feature can optionally use the WOL feature to wake target systems that are in low power mode so they can be configured. A system can be remotely powered up if it is equipped with a WOL-enabled NIC or it has ACPI support in the operating system. Refer to the target ProLiant server documentation to determine if Remote WakeUp is supported by the server.

Replicate Agent Settings Events

Replicate Agent Settings events are used to show the status of a Replicate Agent Settings task. They reflect successful or unsuccessful attempts of a Replicate Agent Settings task execution. They are logged in the job details for the corresponding Replicate Agent Settings task.

Related Procedure

- Creating a Replicate Agent Settings Task

Related Topics

- Replicate Agent Settings
- About Secure Task Execution
- Replicating Trusted Certificates

RPM Package Manager

The RPM Package Manager (RPM) is a powerful command-line driven package-management system capable of installing, uninstalling, verifying, querying, and updating computer software packages. Each software package consists of an archive of files along with information about the package like its version, a description, and the like. There is also a related Application Program Interface (API), permitting advanced developers to bypass shelling out to a command line, and to manage such transactions from within a native coding language. RPM has been integrated into HP Systems Insight Manager (HP SIM) through the **Deploy** menu.

The following procedures are available for RPM within HP SIM:

- **Install RPM.** Refer to “Installing RPM” for more information.
- **Query RPM.** Refer to “Querying RPM” for more information.
- **Uninstall RPM.** Refer to “Uninstalling RPM” for more information.
- **Verify RPM.** Refer to “Verifying RPM” for more information.

Related Procedures

- Installing RPM
- Querying RPM
- Uninstalling RPM
- Verifying RPM

Installing RPM

Use this tool to install RPM Package Manager (RPM) on multiple Linux systems.

To install RPM:

1. Select **Deploy>RPM Package Manager>Install RPM**.
2. Select the target systems. Refer to “Creating a Task” for more information on selecting target systems.
3. Click **Next**. The **Step 2: Specify Parameters** page appears.
4. Enter the parameter, **[install-options] package-file**.

5. Click **Run Now** to run the tool, click **Previous** to return to the previous screen, or click **Schedule** to schedule when the task runs. Refer to “Scheduling a Task” for more information on scheduling the task.

Related Procedures

- Querying RPM
- Uninstalling RPM
- Verifying RPM

Related Topic

- RPM Package Manager

Uninstalling RPM

Use this tool to uninstall RPM Package Manager (RPM) on multiple Linux systems.

To uninstall RPM:

1. Select **Deploy->RPM Package Manager->Uninstall RPM**.
2. Select the target systems. Refer to “Creating a Task” for more information on selecting target systems.
3. Click **Next**. The **Step 2: Specify Parameters** page appears.
4. Enter the parameter, **[erase-options] package-name**.
5. Click **Run Now** to run the tool, click **Previous** to return to the previous screen, or click **Schedule** to schedule when the task runs. Refer to “Scheduling a Task” for more information on scheduling the task.

Related Procedures

- Querying RPM
- Installing RPM
- Verifying RPM

Related Topic

- RPM Package Manager

Querying RPM

This option is used to list installed RPM Package Manager (RPM) package versions and can be run on multiple Linux systems.

To query RPM package version:

1. Select **Deploy->RPM Package Manager->Query RPM**.
2. Select the target systems. Refer to “Creating a Task” for more information on selecting target systems.

3. Click **Next**. The **Step 2: Specify Parameters** page appears.
4. Enter the parameter, **[query-options] package-name**.
5. Click **Run Now** to run the tool, click **Previous** to return to the previous screen, or click **Schedule** to schedule when the task runs. Refer to “Scheduling a Task” for more information on scheduling the task.

Related Procedures

- Installing RPM
- Uninstalling RPM
- Verifying RPM

Related Topic

- RPM Package Manager

Verifying RPM

This tool enables you to verify installed RPM Package Manager (RPM) packages installed and be ran on multiple systems.

To verify RPM:

1. Select **Deploy->RPM Package Manager->Install RPM**.
2. Select the target systems. Refer to “Creating a Task” for more information on selecting target systems.
3. Click **Next**. The **Step 2: Specify Parameters** page appears.
4. Enter the parameter, **[select-options] package-name**.
5. Click **Run Now** to run the tool, click **Previous** to return to the previous screen, or click **Schedule** to schedule when the task runs. Refer to “Scheduling a Task” for more information on scheduling the task.

Related Procedures

- Querying RPM
- Installing RPM
- Uninstalling RPM

Related Topic

- RPM Package Manager

Server Migration Pack

The HP ProLiant Essentials Server Migration Pack (SMP) extends the functionality of the HP ProLiant Essentials Virtual Machine Management Pack (VMM) to provide integrated physical-to-virtual machine (P2V) and virtual-to-virtual machine (V2V) migrations and virtual machine-to-physical (v2P).

SMP enables you to simplify the server consolidation process, thereby freeing you to focus on other priorities. You must have administrative configuration rights to access SMP related menu items.

Go to **Options->Virtualization Management->Upload Drivers** and ensure that all of the necessary binary files have been loaded onto the server. Then you can perform P2V, V2V, or V2P from the **Deploy->Virtual Machine** menu items.

The SMP is a companion product that works in conjunction with an equivalent version of the Virtual Machine Management Pack.

SMP Licensing

SMP uses HP ProLiant Essential products licensing. One license is used for each successful P2V and V2V migration.

To add SMP licenses:

1. To access the **Manage Keys** page, select **Deploy->License Manager->Manage Keys**. The **Manage keys** window is displayed.
2. Click **Add Key**. Refer to “Adding Key Individually” for more information.

Related Procedures

- Accessing the Server Migration Pack
- Adding Key Individually

Accessing the Server Migration Pack

The physical-to-virtual machine (P2V) and virtual-to-virtual machine (V2V) migrations can only be performed if at least one HP ProLiant Essentials Server Migration Pack (SMP) license is available.

To access SMP:

1. Select **Tools->Integrated Consoles->Server Migration Pack**. The **Server Migration Pack** page appears.
2. Select **Migration Options** to perform P2V or V2V migration.

Related Topic

- Server Migration Pack

System Management Homepage

HP Systems Insight Manager (HP SIM) enables you to access the System Management Homepage of a system. The System Management Homepage (SMH) is a Web-based application that provides a consolidated interface for single system management. By aggregating the data from HP Web-based agents and management utilities, the System Management Homepage provides a common, easy-to-use interface for displaying hardware fault & status monitoring, performance data, system thresholds, diagnostics, and software version control for an individual server.

The System Management Homepage can be installed on Windows and Linux operating systems. On IA-32, the Setup Wizard performs the installation of the System Management Homepage and enables you to set the security options used by all of the Web Agents on the system. On Linux Itanium Processor Family (IPF), the System Management Homepage can be installed with default settings through a Red Hat Package Manager (RPM) package, and configured by the **smhconfig** tool.

The System Management Homepage Replicate Agent Settings feature enables HP SIM to retrieve a set of configuration data from HP Web-enabled System Management Software on a reference system and distribute that configuration data to one or more target systems. In addition, some System Management Homepage parameters are replicable through HP SIM. Refer to “Creating a Replicate Agent Settings Task” for more information regarding Replicate Agent Settings.

Related Procedure

- Accessing the System Management Homepage

Related Topic

- System Page

Accessing the System Management Homepage

To access System Management Homepage:

1. Select **Tools->System Information->System Management Homepage**.
2. Select target systems. Refer to “Creating a Task” for more information. The System Management Homepage appears.

Related Procedures

- Creating a Replicate Agent Settings Task
- Accessing the Version Control Agent
- Accessing the Version Control Repository Manager

Related Topics

- System Page
- System Management Homepage

System Page

The **System Page** is used to display information that is related to a specific system. This page displays:

- **Identity Tab**. Includes general system and status information
- **Tools & Links Tab**. Includes links to System Management pages, HP Systems Insight Manager (HP SIM) pages, and other useful links
- **Events Tab**. Displays the event table view page for the system

There are two ways to access the **System Page**:

- Select **Tools->System Information->System Page**. Then select target systems.
- Click the system name in the **System Name** column on the system table view page.

Related Topics

- System Table View Page
- Tools & Links Tab
- Navigating the Event Table View Page
- Identity Tab for Servers
- Identity Tab for Clusters
- Identity Tab for a Complex
- Identity Tab for Partitions
- Identity Tab for a Tape Library
- Identity Tab for a Storage Switch
- Identity Tab for a Storage Host
- Identity Tab for a Storage Array

Identity Tab for Servers

On the **Identity** tab, a status icon indicates the overall health status that is stored in the database. If a system is suspended, a disabled icon appears in place of the hardware status icon and software status icon. The **System Status** section contains more information on the system status.

The **Identity** page is divided into the following sections:

- "System Status"
- "More Information"
- "Identification"
- "Product Description"
- "Contact Information"
- "Asset Information"
- "Management Processor"
- "Associations"

System Status

This section includes:

- **Health Status.** The overall status for a system. It is obtained from Web-Based Enterprise Management (WBEM) Simple Network Management Protocol (SNMP), Desktop Management Interface (DMI) Status Polling tasks, or all three. A ping (ICMP or TCP reachable check) is always made. Click the **Health Status** link to access System Management Homepage (SMH) if present or if it is not, the link accesses the **Property Page Status** page. If noption is available, the **Health Status** link is not present.
- **Management Processor Status.** The management processor status (if available) links to a Web server on the management processor.
- **Software Status.** The software status icon links to the system software Version Control Agent if available.
- **Disabled Status.** A system that is suspended has a disabled icon in the **HW** and **SW** columns on the system table view page.

Note:



If a system is currently in a suspended mode, the **System Page** displays a disclaimer under **System Status** stating `Monitoring of the system is suspended until` and gives a date and time for monitoring to resume.

Partner applications might have their own status registered with the central management server (CMS). If so, these statuses are displayed under **Health Status** and as status columns on the system table view page. For example, the **System Security Vulnerability Status** links to a detailed information about the system status with regard to Vulnerability and Patch Management Pack.

Refer to “System Status Types” for more information on system status types.

More Information

This section provides more detailed information about the system and lists all system information tools available for the system. The available links are:

- **System Management Homepage.** SMH is launched if available
- **Property Page.** The **Property** pages are launched if available
- **Partition Manager View.** The Partition Manager is launched if available
- **Virtual Manager Host View.** The Virtual Manager Host View (VMM) is launched if available

Identification

This section is expanded whenever you access the **System Page** the first time.

Note:



This section can be expanded or collapsed by clicking  and .

Important:



DMI identification is only supported on Windows and HP-UX-based central management server (CMS) installs. In addition, only like operating systems can be identified. For example, Windows-based CMSs can identify Windows-based DMI, and HP-UX-based CMSs can only identify HP-UX-based DMI systems.

The items available in this section include:

- **Address.** The IP address, IPX address, or both that have been discovered for the system.

- **Preferred System Name.** This is the name shown for the system. When available, it defaults to the host name from DNS. You can override this through the **Edit System Properties** link under the **Tools & Links** tab.
- **Network Name.** If available, this is the fully qualified DNS name. Reverse DNS lookups by IP address must be enabled and match a forward lookup.
- **UUID.** This is a unique identifier from the agent or other instrumentation on the system.
- **Serial Number.** This is the serial number of the system.

Why is the device named 'orphan_nnn'?

A system described as an orphan system is a system for which HP Systems Insight Manager (HP SIM) detects that both the IP address and name have been reallocated to another system. Occasionally, this reallocation can happen through simultaneous DHCP address assignment changes and a system re-name. However, the most common cause is from using drive imaging software, such as Altiris. When imaging systems, a globally unique identifier is used by the Web Agents and HP SIM for identification purposes. On Windows systems, this problem can be avoided by deleting the registry key entry, `HKEY_LOCAL_MACHINE\Software\Compaq\CIMAgent\GUID`, from the registry before creating the image. For systems that have already been imaged, stop the foundation agents, remove the key, and restart the agents. A new discovery corrects the problem. Delete any old 'ORPHAN' systems from the HP SIM system list.

Product Description

Note:



This section can be expanded or collapsed by clicking  and .

This section includes:

- **Product ID.** This is the identification number that when added to the serial number of the server, enables HP Support to uniquely identify HP systems.
- **System Type.** This is the basic system type returned from identification.
- **System Subtype.** This is the system subtype returned from identification.
- **Product Model.** This is the product model (name) as defined by the manufacturer.
- **Hardware Description.** This is the description of the hardware obtained from the **Edit System Properties** page.
- **OS Name.** This is the longer operating system name for the system and is used for filtering in operating system-based system collections.
- **OS For Tool Filtering.** This is the short name of the operating system used for tool filter definition files.

- **OS Description.** This is the detailed description of the operating system. For example, service pack information.
- **OS Version.** This is the numerical representation of the operating system version.
- **Management Protocols.** This is the management protocols that have responded when attempting to identify the system.
Note: If more protocols are expected, verify the credentials configured on the **System Protocol Settings** page.
- **Server Role.** This is a user settable server role from the ProLiant agents and can be set from the System Management Homepage.
- **Comments.** This is user settable comments from the SNMP or other agents.
- **Current Running Applications.** This is a list of all applications currently running on the system.

Contact Information

This section includes:

- **Location.** This is a user settable field from the agents for the physical location of the system.
- **Contact.** This is the user settable contact of the system from the agents.

Note: Many of the fields in the contact and product description sections can be overridden locally on the CMS through the **Edit System Properties** pages. Refer to “Editing System Properties for a Single System” for more information.

Asset Information

This section includes **Asset Number**, which is the asset number of the system.

Management Processor

This section appears only if a management processor is available. It includes:

- **Name.** This is the display name (Preferred Name) of the management processor used to manage the system.
- **Address.** This is the IP address of the management processor used to manage the system.
- **Model.** This is the model name of the management processor for this system.

Associations

This section includes:

- **Enclosure Name.** This is the name of the enclosure, if the system is in an enclosure, for example, a p-Class server blade.
- **Rack Name.** This is the name of the rack, if the enclosure is in a rack that could be discovered.

- **Slot.** This is the slot number that the system is positioned within the enclosure.
- **Server Dimensions.** If available, this is the dimensions in millimeters of the system.

Related Topics

- System Page
- Tools & Links Tab
- Identity Tab for Virtual Machine Hosts
- Navigating the Event Table View Page

Identity Tab for Management Processors

On the **Identity** tab, a status icon indicates the overall health status that is stored in the database. If a system is suspended, a disabled icon appears in place of the hardware status icon.

The **Identity** page is divided into the following sections:

- “System Status”
- “Identification”
- “Product Description”

System Status

This section includes:

Health Status. The overall status for a system. It is obtained from Web-Based Enterprise Management (WBEM) Simple Network Management Protocol (SNMP), Desktop Management Interface (DMI) Status Polling tasks, or all three. A ping (ICMP or TCP reachable check) is always made. Click the **Health Status** link to access management processor's home page.

Refer to “System Status Types” for more information on system status types.

Identification

This section is expanded whenever you access the **System Page** the first time.

Note:



This section can be expanded or collapsed by clicking  and .

Important:



DMI identification is only supported on Windows and HP-UX-based central management server (CMS) installs. In addition, only like operating systems can be identified. For example, Windows-based CMSs can identify Windows-based DMI, and HP-UX-based CMSs can only identify HP-UX-based DMI systems.

The items available in this section include:

- **Address.** The IP address, IPX address, or both that have been discovered for the system.
- **Preferred System Name.** This is the name shown for the system. When available, it defaults to the host name from DNS. You can override this through the **Edit System Properties** link under the **Tools & Links** tab.
- **Network Name.** If available, this is the fully qualified DNS name. Reverse DNS lookups by IP address must be enabled and match a forward lookup.
- **Serial Number.** This is the serial number of the system.

Product Description

Note:



This section can be expanded or collapsed by clicking  and .

This section includes:

- **System Type.** This is the basic system type returned from identification.
- **Product Model.** This is the product model (name) as defined by the manufacturer.
- **Hardware Description.** This is the description of the hardware obtained from the **Edit System Properties** page.
- **Management Protocols.** This is the management protocols that have responded when attempting to identify the system.

Note: If more protocols are expected, verify the credentials configured on the **System Protocol Settings** page.

Related Topics

- System Page
- Tools & Links Tab
- Navigating the Event Table View Page

Identity Tab for Virtual Machine Hosts

To access the **System Page** for a virtual machine host, click the system name of the host on the **All Systems** page, or click the vm status. The **System Page** appears with the **Identity** tab selected.

The **Identity** tab includes the following information:

- **Virtual Machine.** The virtual machine status, virtual machine state, system name, virtual machine name, IP address, and virtual machine operating system are included in this section.

- **Identification.** This section includes the address, preferred system name, and network name of the VM guest. Refer to “Identity Tab for Servers” for more information on these fields.
- **Product Description.**
 - **System Type.** This is the basic system type returned from identification.
 - **System Subtype.** This is the system subtype returned from identification.
 - **Hardware Description.** This is the description of the hardware obtained from the **Edit System Properties** page.
 - **OS Name.** This is the longer operating system name for the system and is used for filtering in operating system-based system collections.
 - **OS For Tool Filtering.** This is the short name of the operating system used for tool filter definition files.
 - **OS Description.** This is the detailed description of the operating system. For example, service pack information.
 - **OS Version.** This is the numerical representation of the operating system version.
 - **Management Protocols.** This is the management protocols that have responded when attempting to identify the system.
Note: If more protocols are expected, verify the credentials configured on the **System Protocol Settings** page.
 - **Virtualization.** The type of virtualization software installed and also links to the remote console.
- **Virtual machine.** The virtual machine status, system name, virtual machine name, IP address, and virtual machine operating system.

Note:



Depending on the host configuration, additional details might be displayed.

Related Topics

- System Page
- VM Performance Tab for Hosts
- Identity Tab for Virtual Machine Guests
- Virtual Machine Management Pack
- Identity Tab for Servers

Identity Tab for Virtual Machine Guests

To access the **System Page** for a virtual machine guest, click the system name of the guest on the **All Systems** page. The **System Page** appears with the **Identity** tab selected.

The **Identity** tab includes the following information:

- **System status.** This section includes:
 - **Health Status.** The overall status for a system. It is obtained from Web-Based Enterprise Management (WBEM) Simple Network Management Protocol (SNMP), Desktop Management Interface (DMI) Status Polling tasks, or all three. A ping (ICMP or TCP reachable check) is always made. Click the **Health Status** link to access System Management Homepage (SMH) if present or if it is not, the link accesses the **Property Page Status** page. If no option is available, the **Health Status** link is not present.

Refer to “System Status Types” for more information on the system status types.
 - **Vulnerability status.**
 - **Virtual Machine Management Status.** The status of the Virtual Machine (VM) status.

Refer to “VM Status Types” for more information on the VM status types.

- **Virtual Machine Controls.** There are several actions that you can take from this page. They include: launching the remote console, and starting, stopping, resetting, and pausing the VM guest.

- **Identification.** This section includes the address, preferred system name, and network name of the VM guest. Refer to “Identity Tab for Servers” for more information on these fields.

- **Product Description.** This section includes the following information:
 - **System Type.** This is the basic system type returned from identification.
 - **System Subtype.** This is the system subtype returned from identification.
 - **Hardware Description.** This is the description of the hardware obtained from the **Edit System Properties** page.
 - **OS Name.** This is the longer operating system name for the system and is used for filtering in operating system-based system collections.
 - **OS For Tool Filtering.** This is the short name of the operating system used for tool filter definition files.
 - **OS Description.** This is the detailed description of the operating system. For example, service pack information.
 - **OS Version.** This is the numerical representation of the operating system version.
 - **Management Protocols.** This is the management protocols that have responded when attempting to identify the system.

Note: If more protocols are expected, verify the credentials configured on the **System Protocol Settings** page.

- **Virtual Machine Configuration Details.** This section includes configuration details including:
 - **VM Host.** The system name of the VM host.
 - **Virtualization.** The virtualization technology installed on the VM host.
 - **Configuration File.** The name and location of the configuration file.
 - **Configuration Folder.** The name and location of the configuration folder.
 - **Memory.** The memory on the VM host.
 - **Virtual Disk.** The type of virtual disk.
 - **CD/DVD RM.** Includes details about the CD/DVD drive.
 - **Floppy Drive.** Identity of the floppy drive.
 - **Network Card.** Includes details about the network card.
 - **Total File Size.** The total file size of the VM host.

Related Procedures

- Virtual Machine Controls - Launching the Remote Console
- Virtual Machine Controls - Starting the Virtual Machine
- Virtual Machine Controls - Stopping the Virtual Machine
- Virtual Machine Controls - Pausing the Virtual Machine
- Virtual Machine Controls - Resetting the Virtual Machine

Related Topics

- System Page
- VM Performance Tab for Guests
- Identity Tab for Virtual Machine Hosts
- Virtual Machine Management Pack

Virtual Machine Controls - Launching the Remote Console

You can launch the Virtual Machine (VM) remote console from the **System Page, Identity** tab.

Important:



Microsoft Virtual Server 2005 remote console is only supported with Microsoft Internet Explorer browsers. VMware Management Interface must be installed on VMware GSX Server VM hosts to launch the remote console. If you are launching

a remote console from a VMware host, VMware Remote Console application must be installed on the system from which you are launching remote console.

To launch the VM remote console:

1. Select **Tools->System Information->System Page**.
2. Select a VM host or guest. Refer to “Creating a Task” for more information on selecting a target system.
3. Click **Launch Remote Console**.

Related Procedures

- Virtual Machine Controls - Starting the Virtual Machine
- Virtual Machine Controls - Stopping the Virtual Machine
- Virtual Machine Controls - Pausing the Virtual Machine
- Virtual Machine Controls - Resetting the Virtual Machine

Related Topics

- System Page
- Identity Tab for Virtual Machine Guests
- VM Performance Tab for Guests

Virtual Machine Controls - Starting the Virtual Machine

You can start or resume a Virtual Machine (VM) host or guest from the **System Page, Identity** tab.

Note:



A Virtual Machine (VM) guest can only be started or resumed if it is currently stopped, shut down, or paused.

To start or resume a VM guest:

1. Select **Tools->System Information->System Page**.
2. Select a VM host or guest. Refer to “Creating a Task” for more information on selecting a target system.
3. Click **Start**. A confirmation box appears.
4. Click **OK** to confirm the process.

If the VM guest is currently stopped or paused, the guest is started or resumed. If the VM guest is currently suspended to disk (only possible with Microsoft Virtual Server 2005), selecting **Resume Virtual Machine Guest** restores the VM guest to the previous state and powers on the VM guest.

When the power-on process is complete, the status is updated to a Normal status. The **Start** button is displayed, and the **Stop**, **Pause**, and **Reset** buttons are enabled.

If a VM guest becomes stuck during the start process, the HP ProLiant Essentials Virtual Machine Management Pack (VMM) displays **User Intervention** and the status is updated to Major.

Related Procedures

- Virtual Machine Controls - Launching the Remote Console
- Virtual Machine Controls - Stopping the Virtual Machine
- Virtual Machine Controls - Pausing the Virtual Machine
- Virtual Machine Controls - Resetting the Virtual Machine

Related Topics

- System Page
- Identity Tab for Virtual Machine Guests
- VM Performance Tab for Guests

Virtual Machine Controls - Resetting the Virtual Machine

You can reset a Virtual Machine (VM) guest from the **System Page**, **Identity** tab.

To reset a VM guest:

1. Select **Tools->System Information->System Page**.
2. Select a VM guest. Refer to “Creating a Task” for more information on selecting a target system.
3. Click **Reset**. A confirmation box appears.
4. Click **OK** to confirm the process.

Selecting **Reset** powers off and then powers on the VM guest. Selecting **Restart** shuts down the VM guest operating system and then powers off and powers on the VM guest.

Caution:



Unsaved data is lost if you click **Reset**.

The VM status is updated to Normal. The **Start** button is disabled, and the **Stop**, **Pause**, and **Reset** buttons are disabled, and the **Start** buttons are enabled.

Related Procedures

- Virtual Machine Controls - Starting the Virtual Machine
- Virtual Machine Controls - Stopping the Virtual Machine
- Virtual Machine Controls - Pausing the Virtual Machine
- Virtual Machine Controls - Launching the Remote Console

Related Topics

- System Page
- Identity Tab for Virtual Machine Guests
- VM Performance Tab for Guests

Virtual Machine Controls - Pausing the Virtual Machine

You can pause a Virtual Machine (VM) guest from the **System Page, Identity** tab.

Note:



A VM guest can only be paused if it is currently powered on and running.

To pause a VM guest:

1. Select **Tools->System Information->System Page**.
2. Select a VM guest. Refer to “Creating a Task” for more information on selecting a target system.
3. Click **Pause**. A confirmation box appears.
4. Click **OK** to confirm the process.

For Microsoft Virtual Server 2005 VM guests, select **Suspend to disk** or **Pause VM** when prompted. Selecting **Suspend to disk** saves the current state and then pauses the VM guest. Selecting **Pause VM** suspends the VM guest without discarding the state

The VM status is updated to Disabled. The **Stop**, **Pause**, and **Reset** buttons are disabled, and the **Start** button is enabled.

Related Procedures

- Virtual Machine Controls - Starting the Virtual Machine
- Virtual Machine Controls - Stopping the Virtual Machine
- Virtual Machine Controls - Launching the Remote Console
- Virtual Machine Controls - Resetting the Virtual Machine

Related Topics

- System Page
- Identity Tab for Virtual Machine Guests
- VM Performance Tab for Guests

Virtual Machine Controls - Stopping the Virtual Machine

You can shut down or stop a Virtual Machine (VM) guest from the **System Page, Identity** tab.

Note:



A VM guest can only be shut down if it is currently powered on and the Microsoft Virtual Server Additions of the VMware Tools are installed on the VM guest.

To shut down or stop a VM guest:

1. Select **Tools->System Information->System Page**.
2. Select a VM guest. Refer to "Creating a Task" for more information on selecting a target system.
3. Click **Stop**. A confirmation box appears.
4. Click **OK** to confirm the process.
5. Select **Stop VM** or **Shut down VM** when prompted. Selecting **Stop VM** powers off the VM guest immediately without saving the current state. Selecting **Shut down VM** shuts down the VM operating system and then powers off the VM guest.

Caution:



Unsaved data is lost if you select **Stop VM**.

When you stop or shut down the VM guest, the VM guest status is updated to Disabled. The **Stop**, **Pause**, and **Reset** buttons are disabled and the **Start** button is enabled.

Related Procedures

- Virtual Machine Controls - Starting the Virtual Machine
- Virtual Machine Controls - Launching the Remote Console
- Virtual Machine Controls - Pausing the Virtual Machine
- Virtual Machine Controls - Resetting the Virtual Machine

Related Topics

- System Page
- Identity Tab for Virtual Machine Guests
- VM Performance Tab for Guests

VM Performance Tab for Hosts

After clicking a Virtual Machine (VM) host from the **All Systems** page, select the **VM Performance** tab to display the performance information for the VM host. Activity for the most recent 1, 5, fifteen, thirty, or sixty minutes can be displayed. If the amount of time requested exceeds the amount available, all available information is reported.

- **VM Host Performance.** This section includes:
 - **Processor Utilization Percentage.** The processor utilization on the VM host
 - **VM Processor Utilization Percentage.** The processor consumption by all of the VMs on the host
 - **Reserved Capacity (All running VMs).** The sum of the Reserved System Capacity values for all VMs currently powered on. This is for Microsoft Virtual Server 2005 VM hosts only.
 - **CPU Min (All running VMs).** The sum of the CPU min values for all VMs currently powered on divided by the resources available on the host. This is for VMware ESX Server only.
 - **Memory Utilization.** The total amount of memory currently in use on the host, based on memory utilization relative to the amount of physical memory configured on the host.
 - **VM Memory.** The total amount of memory currently in use by VMs executing on the host, based on the VM utilization relative to the amount of physical memory configured.
 - **Network Throughput.** The network traffic transmitted and received on the host. The bar is always filled completely.
 - **Network Transmission Throughput.** The network traffic transmitted by the host and all VMs on the host. The bar represents the transmission percentage of the network throughput.
 - **Storage Throughput.** The storage read and written by the host and all VMs on the host. The bar represents the read percentage of storage throughput.
 - **Storage Write Throughput.** The storage written by the host and all VMs on the host. The bar represents the write percentage of storage throughput.
- **Threshold Settings.** A VM host-specific threshold can be evaluated.
 - **Threshold Interval.** The number of minutes of utilization data that must be available before the threshold is evaluated.
 - **Threshold Value.** The maximum utilization value that provides a normal status.

- **Measured Interval.** The number of minutes of utilization data averaged to calculate the measured value.
- **Measured Value.** The average utilization over the most recent measured interval.
- **State.** The current state of the threshold. The can be:
 - **Unknown.** Indicates that the number of utilization samples available is less than the Threshold Interval.
 - **Normal.** Indicates that sufficient utilization samples are available, and the Measured Value is less than or equal to the Threshold Value.
 - **Exceeded.** Indicates that sufficient utilization samples are available, and the Measured Value is greater than the Threshold Value.
- **Virtual Machine Performance.** This section displays the value averages that are relative to the duration of the VM host activity. The following values are displayed for each VM on the host.
 - **CPU.** The CPU percentage consumed by the VM relative to the total processor capacity of the VM host.
 - **vCPU.** The CPU percentage consumed by the VM relative to its resource allocation.
 - **Memory.** The physical host memory currently in use by the VM.
 - **Network.** The network throughput for the VM. The bar indicates the VM network throughput as a percentage of the total network throughput on the VM host.
 - **Storage.** The storage throughput for the VM. The bar indicates the VM storage throughput as a percentage of the total storage throughput on the VM host.

Related Topics

- System Page
- Identity Tab for Virtual Machine Hosts
- VM Performance Tab for Guests
- Virtual Machine Management Pack

VM Performance Tab for Guests

After clicking a Virtual Machine (VM) guest on the **All Systems** page, select the **VM Performance** tab to display the following configuration information for the guest:

- **VM Performance.** This section includes:
 - **Processor Utilization Percentage.** The processor utilization on the VM host.
 - **VM Processor Utilization (vCPU).** The CPU percentage consumed by the VM relative to the resource utilization.

- **Host Processor Utilization on x CPUs.** The CPU percentage consumed by the VM relative to the number of physical processors (x) on which the VM can execute.
- **Host Processor Utilization on all CPUs.** The CPU consumed by the VM relative to the total VM Host Processors.
- **Memory Utilization.** The physical host used by the VM.
- **Network Throughput.** The network traffic transmitted and received by the VM. The bar is always completely filled.
- **Network Transmission Throughput.** The network traffic transmitted by the VM. The bar represents the transmission percentage of the Network Throughput.
- **Network Receive Throughput.** The network traffic received by this VM. The bar represents the receive percentage of the VM Network Throughput.
- **Storage Throughput.** The storage read and written by VM. The bar represents the read percentage of Storage Throughput.
- **Storage Read Throughput.** The storage read by the VM/ The bar represents the read percentage of the Storage Throughput.
- **Storage Write Throughput.** The storage written by the VM. The bar represents the write percentage of Storage Throughput.
- **Resource Allocation.** The bars indicate the VM allocation relative to the capacity available on the VM host.
 - **VMware ESX Server VMs.** This section includes:
 - **CPU Min.** The cpu.min value reported by ESX.
 - **CPU Max.** The cpu.max value reported by ESX.
 - **CPU Shares.** The cpu.shares value reported by ESX.
 - **Microsoft Virtual Server 2005 VMs.** This section includes:
 - **Reserved Capacity.** The reserved system capacity value reported by the virtual server relative to one CPU.
 - **Maximum Capacity.** The maximum system capacity value reported by the virtual server relative to one CPU.
 - **Relative Weight.** The relative weight value reported by the virtual server.
- **Threshold Settings.** A VM-specific threshold can be evaluated and this section includes:
 - **Threshold Interval.** The number of minutes of utilization data that must be available before the threshold is evaluated.
 - **Threshold Value.** The maximum utilization value that provides a normal status.

- **Measured Interval.** The number of minutes of utilization data that is averaged when calculating the Measured Value.
- **Measured Value.** The average utilization over the most recent Measured Interval minutes.
- **State.** The current state of the threshold. The state can be:
 - **Unknown.** Indicates that the number of utilization samples available is less than the Threshold Interval.
 - **Normal.** Indicates that sufficient utilization samples are available, and the Measured Value is less than or equal to the Threshold Value.
 - **Exceeded.** Indicates that sufficient utilization samples are available, and the Measured Value is greater than the Threshold Value.

Related Topics

- System Page
- Identity Tab for Virtual Machine Guests
- VM Performance Tab for Hosts
- Virtual Machine Management Pack

Identity Tab for Clusters

Based on the type of cluster provider and the version of cluster providers, not all properties are available at all times. If a property does not have a value, the property does not appear on this page. This page is for all clusters except for MSCS clusters. They are monitored using Cluster Monitor. Refer to “Cluster Monitor” for more information.

Health Status

Each link under **Health Status**, links to the **System Page** of a cluster member. The cluster status is a combination of the cluster member statuses included in the cluster. The most critical status is displayed.

Identification

- **Address.** This is the IP address of the cluster.
- **Preferred System Name.** This is the name shown for the system. When available, it defaults to the host name from DNS. You can override this through the **Edit System Properties** link under the **Tools & Links** tab.
- **Network Name.** If available, this is the fully qualified DNS name. Reverse DNS lookups by IP address must be enabled and match a forward lookup.

Product Description

Note:



This section can be expanded or collapsed by clicking  and .

- **Cluster Name.** This is the name of the cluster.
- **System Type.** This is the basic system type returned from identification
- **Cluster Type.** This is the basic cluster type returned from identification.
- **Product Model.** This is the product model (name) as defined by the manufacturer.
- **OS Name.** This is the longer operating system name for the system and is used for filtering in operating system-based system collections.
- **OS For Tool Filtering.** This is the short name of the operating system used for tool filter definition files.
- **Management Protocols.** This is the management protocols that have responded when attempting to identify the system.

Note: If more protocols are expected, verify the credentials configured on the **System Protocol Settings** page.

Related Topics

- System Page
- Identity Tab for Servers

Identity Tab for a Complex

A complex is a container type system and contains nPartitions. Additional links are available on the **System Page** to access detailed information when a complex system is selected. Included here are the areas that are unique to a complex. Refer to “Identity Tab for Servers” for additional information about the tab.

Health Status

Each link under **Health Status**, links to the **System Page** of a partition. The health status of a complex is a combination of all the health statuses of each partition included in the complex. The most critical status is displayed.

Product Description

Note:



This section can be expanded or collapsed by clicking  and .

This section includes the following information:

- **Complex Name.** This is the name of the complex returned from identification.
- **Product Name.** This is the product name as defined by the manufacturer.
- **Serial Number.** The serial number of the complex returned from identification.
- **Product Number - Current.**
- **Product Number - Original.**
- **Complex Profile Revision.**
- **Active Service Processor Location.**

Summary of Components

For a Complex Participating in iCOD

- **Computer Cabinets.**
- **I/O Cabinets.**
Need text here
- **nPartitions.** This is partition of an HP server, comprising a group of cells (containing CPUs and memory) and I/O chassis (containing I/O systems).
- **Licensed Cells.**
- **Unlicensed/iCOD Cells.**
- **Licenses Processors.**
- **Unlicensed/iCOD Processors.**
- **DIMMs.** This is the Dual In-line Memory Module memory chips installed.
- **Licensed Memory (GB).**
- **Unlicensed/iCOD Memory (GB).**
- **Chassis.**
- **I/O Cards.**

- **iCOD.**
- **iCOD Balance.**

For a Complex Not Participating in iCOD

- **Computer Cabinets.**
- **I/O Cabinets.**
- **nPartitions.**
- **Cells.**
- **CPUs.**
- **DIMMs.**
- **Memory (GB).**
- **I/O Chassis.**
- **I/O Cards.**
- **iCOD.**

Related Topics

- System Page
- Identity Tab for Servers
- Identity Tab for Partitions

Identity Tab for Partitions

The **System Page** for a partition follows the same layout as a server **System Page**. However, it is extended to include unique information that applies to partitions only.

The following sections include only the unique information for a partition. Refer to “Identity Tab for Servers” for additional information about the tab.

Identification

The **Identification** section is expanded whenever you access the **System Page** for the first time. The items available under this section include:

- **nPartition Name.**
- **nPartition Number.**
- **Host Name.**

Product Description

Note:



This section can be expanded or collapsed by clicking  and .

- **CPU Architecture.**
- **Cell Compatibility.**
- **Firmware Revision.**
- **Primary Boot Path.**
- **HA Alternate Boot Path.**
- **Alternate Boot Path.**

Summary of Components

- **Active Cells.**
- **Inactive Cells.**
- **Active Processors.**
- **Inactive Processors.**
- **Number of Licensed Processors.**

Only available for partitions that participate in Instand Capacity.

- **DIMMs.**
- **Memory (GB).**
- **I/O Chassis.**
- **I/O Cards.**

Associations

- **Complex Name.**

Related Topics

- System Page
- Identity Tab for Servers
- Identity Tab for a Complex

Identity Tab for a Storage Host

A storage host is a server, desktop, or workstation that is connected by a host bus adapter (HBA) to a storage area network (SAN). Additional links are available on the **System Page** to access detailed information when a storage host is selected. Included here are the areas that are unique to storage hosts. HP SIM displays data supplied by each HBA's SMI-S provider. If an HBA's SMI-S provider does not supply data for a particular property, the property does not appear on this page. Refer to "Identity Tab for Servers" for additional information about the tab.

The Host Bus Adapters section shows the date, time, and duration of the last data collection task. If you want to update the data, click the **Last Update** link, and schedule or run a Data Collection task. Refer to "Data Collection" for additional information about data collection tasks.

If this host is managed by HP Storage Essentials, the **Host Bus Adapters** and **LUNs** sections do not appear on this page, and an **SE System Properties** link appears in the **Storage Essentials Pages** section on the **Tools & Links** tab. Click the **SE System Properties** link to view the Storage Essentials device page for this storage host.

Product Description

Note:



This section can be expanded or collapsed by clicking  and .

In addition to the Product Description information on the "Identity Tab for Servers", this section may include:

System Subtype. Storage systems use the following subtypes:

- **Storage.** A system that is identified as part of the storage infrastructure.
- **SMI.** A system that was discovered through an SMI-S provider.
- **Storage Essentials Managed.** A system that is managed by HP Storage Essentials.

Note:



If a system is managed by HP Storage Essentials, it does not show the **SMI** subtype.

Host Bus Adapters

Note:



This section can be expanded or collapsed by clicking  and .

This section lists the installed Fibre Channel HBAs.

- **Element Name.** The name of the HBA.
- **WWN.** The node world wide name of the HBA.
- **Status.** The HBA's WBEM operational status. Refer to “WBEM Operational Status Types” for additional information about WBEM status.

Note:



Click  to view HBA property and port information.

Properties

Note:



This section can be expanded or collapsed by clicking  and .

-
- **Product Name.** The product name for the HBA, for example, a model number.
 - **Product Vendor.** The HBA vendor.
 - **Product Identifying Number.** A unique identifier for the HBA, for example, a serial number.
 - **Product Version.** The HBA product version.
 - **Driver Version.** The installed HBA driver version.
 - **Driver Manufacturer.** The manufacturer of the HBA driver.
 - **Firmware Version.** The installed HBA firmware version.
 - **Firmware Manufacturer.** The HBA firmware manufacturer.

- **BIOS/FCode Version.** The installed BIOS/FCode version.
- **BIOS/FCode Manufacturer.** The BIOS/FCode manufacturer.

Ports

Note:



This section can be expanded or collapsed by clicking  and .

-
- **Element Name.** The port number.
 - **WWN.** The port's world wide name.
 - **Port Type.** The port type. Refer to "Port Types" for additional information.
 - **Status.** The port's WBEM operational status. Refer to "WBEM Operational Status Types" for additional information about WBEM status.

LUNs

Note:



This section can be expanded or collapsed by clicking  and .

This section lists the LUNs in use by the host.

- **LUN Name.** The name of a LUN in use by the selected host.
- **LUN Number.** The number by which the LUN (as seen through this port) is known to the storage host.
- **Storage Device.** The name of the storage device that contains the listed LUN. Click the storage device name to view the storage device **System Page**.

A link from a LUN to a storage device appears in this column only if the LUN is reported by the SMI-S provider of the storage array on which the LUN resides, and is reported with the same Name property used by the HBA's SMI-S provider. If these conditions are not met, but the HBA's SMI-S provider reports the LUN, the LUN's storage device is listed as **Unknown**.

- **HBA Name.** The name of the HBA that connects the host to the LUN.
- **Port WWN.** The port number through which the host connects to the LUN.
- **LUN Size.** The usable size of the LUN.

- **RAID Level.** The LUN's RAID level. RAID level information is available only if a LUN is matched up to a volume on a storage device. Refer to Storage Volumes [useTools_systemPage_identity_storageArray.html#Storage_Volumes] for additional information about RAID levels.

Related Topics

- System Page
- Identity Tab for Servers
- Port Types
- Data Collection

Identity Tab for a Storage Switch

A storage switch is a Fibre Channel switch that is connected to a storage area network (SAN). Additional links are available on the **System Page** to access detailed information when a storage switch is selected. Included here are the areas that are unique to storage switches. HP SIM displays data supplied by the switch's SMI-S provider. If the SMI-S provider does not supply data for a particular property, the property does not appear on this page. Refer to "Identity Tab for Servers" for additional information about the tab.

The Ports and Status Summary sections show the date, time, and duration of the last data collection task. If you want to update the data, click the **Last Update** link, and schedule or run a Data Collection task. Refer to "Data Collection" for additional information about data collection tasks.

If this switch is managed by HP Storage Essentials, the **Ports** and **Status Summary** sections do not appear on this page, and an **SE System Properties** link appears in the **Storage Essentials Pages** section on the **Tools & Links** tab. Click the **SE System Properties** link to view the Storage Essentials device page for this storage switch.

Product Description

Note:



This section can be expanded or collapsed by clicking  and .

In addition to the Product Description information on the "Identity Tab for Servers", this section includes:

- **System Subtype.** Storage systems use the following subtypes:
 - **Storage.** A system that is identified as part of the storage infrastructure.
 - **SMI.** A system that was discovered through an SMI-S provider.
 - **Storage Essentials Managed.** A system that is managed by HP Storage Essentials.

Note:



If a system is managed by HP Storage Essentials, it does not show the **SMI** subtype.

- **Product Name.** The product name for the switch, for example, a model number.
- **Product Vendor.** The switch vendor.
- **Product Identifying Number.** A unique identifier for the switch, for example, a serial number.
- **Product Version.** The switch product version.
- **Firmware Version.** The installed firmware version.
- **Firmware Manufacturer.** The firmware manufacturer.
- **BIOS/FCode Version.** The installed BIOS/FCode version.
- **BIOS/FCode Manufacturer.** The BIOS/FCode manufacturer.
- **Management Proxies.** The server(s) that manage the switch through a management protocol such as WBEM.
- **Software Version.** The version of the software installed on this system.
- **Software Manufacturer.** The manufacturer of the software installed on this system.

Note:



Some vendors enter firmware details in the **Software Version** and **Software Manufacturer** fields instead of the **Firmware Version** and **Firmware Manufacturer** fields. These fields might display data about any software related to the system.

Ports

Note:



This section can be expanded or collapsed by clicking  and .

- **Port Number.** The port number.
- **WWN.** The port's world wide name.

- **Port Type.** The port type. Refer to “Port Types” for additional information about port types.
- **Status.** The port's WBEM operational status. Refer to “WBEM Operational Status Types” for additional information about WBEM status.

Status Summary

Note:



This section can be expanded or collapsed by clicking  and .

This section summarizes the status information in the Ports section.

- **Status.** The WBEM operational status. Refer to “WBEM Operational Status Types” for additional information about WBEM status.
- **Count.** The number of ports with the listed status.

Related Topics

- System Page
- Identity Tab for Servers
- WBEM Operational Status Types
- Port Types
- Data Collection

Identity Tab for a Storage Array

A storage array is a disk array that uses a Fibre Channel controller to connect to a storage area network (SAN). Additional links are available on the **System Page** to access detailed information when a storage array is selected. Included here are the areas that are unique to storage arrays. HP SIM displays data supplied by the array's SMI-S provider. If the SMI-S provider does not supply data for a particular property, the property does not appear on this page. Refer to “Identity Tab for Servers” for additional information about the tab.

The Ports, Storage Volumes, and Capacity Information sections show the date, time, and duration of the last data collection task. If you want to update the data, click the **Last Update** link, and schedule or run a Data Collection task. Refer to “Data Collection” for additional information about data collection tasks.

If this storage array is managed by HP Storage Essentials, the **Ports**, **Storage Volumes**, and **Capacity Information** sections do not appear on this page, and an **SE System Properties** link appears in the **Storage Essentials Pages** section on the **Tools & Links** tab. Click the **SE System Properties** link to view the Storage Essentials device page for this storage array.

Product Description

Note:



This section can be expanded or collapsed by clicking  and .

In addition to the Product Description information on the “Identity Tab for Servers”, this section might include:

- **System Subtype.** Storage systems use the following subtypes:
 - **Storage.** A system that is identified as part of the storage infrastructure.
 - **SMI.** A system that was discovered through an SMI-S provider.
 - **Storage Essentials Managed.** A system that is managed by HP Storage Essentials.

Note:



If a system is managed by HP Storage Essentials, it does not show the **SMI** subtype.

-
- **Product Name.** The product name for the array, for example, a model number.
 - **Product Vendor.** The storage array vendor.
 - **Product Identifying Number.** A unique identifier for the storage array, for example, a serial number.
 - **Product Version.** The array product version.
 - **Firmware Version.** The installed firmware version.
 - **Firmware Manufacturer.** The firmware manufacturer.
 - **BIOS/FCode Version.** The installed BIOS/FCode version.
 - **BIOS/FCode Manufacturer.** The BIOS/FCode manufacturer.
 - **Management Proxies.** The server(s) that manage the selected array through a management protocol, such as WBEM.
 - **Software Version.** The version of the software installed on this system.
 - **Software Manufacturer.** The manufacturer of the software installed on this system.

Note:



Some vendors enter firmware details in the **Software Version** and **Software Manufacturer** fields instead of the **Firmware Version** and **Firmware Manufacturer** fields. These fields might display data about any software related to the system.

Note:



If this storage array is managed by HP Storage Essentials, data is not displayed for the **Product Name**, **Product Vendor**, **Product Identifying Number**, and **Product Version**.

Ports

Note:



This section can be expanded or collapsed by clicking  and .

If HP Systems Insight Manager has discovered controllers that manage this array's ports, they will be displayed as expandable elements in the **Ports** table. If no controllers were discovered, the table lists only port details.

Controller Details

- **Element Name.** The name of the controller.
- **LUN Count.** The number of connections made through this controller.
- **Status.** The controller's WBEM operational status. Refer to “WBEM Operational Status Types” for additional information about WBEM status.

Note:



Click  to view specific port details.

Port Details

- **Element Name.** The port name.
- **WWN.** The port's world wide name.

- **Port Type.** The port type. Refer to “Port Types” for additional information about port types.
- **LUN Count.** The number of connections made through this port.
- **Status.** The port's WBEM operational status. Refer to “WBEM Operational Status Types” for additional information about WBEM status.

Storage Volumes

Note:



This section can be expanded or collapsed by clicking  and .

This section lists the array's storage volumes. Storage volumes are logical volumes on an array, for example, LUNs.

- **Volume Name.** The storage volume name.
- **Visible to Host(s).** The storage volume is accessible to the listed host(s).
- **Block Size.** The storage volume's block size in bytes.
- **Number of Blocks.** The total number of blocks on the storage volume.
- **Total Size.** The storage volume's total size.
- **RAID Level.** The RAID level of the storage volume. Typically, this value is supplied by the array's SMI-S provider. If the SMI-S provider does not supply a value, HP Systems Insight Manager calculates the RAID level based on the values for Package Redundancy and Data Redundancy as follows:

Package Redundancy	Data Redundancy	RAID Level
0	1	RAID 0
1	1	RAID 5
1	2	RAID 1
2	1	RAID 6
2	2	RAID 15/51

If the RAID value is calculated by HP Systems Insight Manager, an asterisk is added to the RAID value, for example **RAID 5***.

Capacity Information

Note:



This section can be expanded or collapsed by clicking  and .

The Capacity Information table lists the hierarchy of available capacity metrics for storage arrays in the **Metric** column, and the corresponding disk space value in the **Size** column. For each metric, the disk space value is expressed as a percentage of the array's raw capacity in the **Percentage of Raw Capacity** column. **Raw Capacity**, the total capacity of the array, is divided into space that is **Un-Allocated** and **Carved for LUNs**. Space that is carved into LUNs is divided into **RAID Overhead**, **Usable bytes assigned to Ports**, and **Bytes not yet assigned to Ports**.

The metrics in the Capacity Information table are also displayed as percentages in a pie chart below the table. If any value in the table shows an **Undetermined** value, the pie chart is not displayed.

- **Un-Allocated.** The total amount of storage on the array that has not been configured.
- **Carved for LUNs.** The total amount of configured storage on the array, including RAID overhead. For example, if 100 gigabytes (GB) is allocated for a RAID-1 (mirrored) storage volume, 50 GB will be usable by the end-user, 50 GB is considered RAID overhead, and 100 GB is considered carved for LUNs.
 - **RAID Overhead.** The total amount of storage on the array that is not directly usable because it is being used to provide redundancy.
 - **Usable bytes assigned to Ports.** The total amount of configured and usable storage on the array that is connected through one or more ports.
 - **Usable bytes not yet assigned to Ports.** The total amount of configured and usable storage on the array that is not connected through any port. Users cannot access this storage until it is assigned to a port.

Related Topics

- System Page
- Identity Tab for Servers
- Port Types
- Data Collection

Identity Tab for a Tape Library

A tape library is a tape drive that is connected to a storage area network (SAN). Additional links are available on the **System Page** to access detailed information when a tape library is selected. Included here are the areas that are unique to tape libraries. HP SIM displays data supplied by the tape library's SMI-S provider. If the SMI-S provider does not supply data for a particular property,

the property does not appear on this page. Refer to “Identity Tab for Servers” for additional information about the tab.

The Ports, Media Access Devices, and Changer Devices sections show the date, time, and duration of the last data collection task. If you want to update the data, click the **Last Update** link, and schedule or run a Data Collection task. Refer to “Data Collection” for additional information about data collection tasks.

If this tape library is managed by HP Storage Essentials, the **Ports, Media Access Devices, and Changer Devices** sections do not appear on this page, and an **SE System Properties** link appears in the **Storage Essentials Pages** section on the **Tools & Links** tab. Click the **SE System Properties** link to view the Storage Essentials device page for this tape library.

Product Description

Note:



This section can be expanded or collapsed by clicking  and .

In addition to the Product Description information on the “Identity Tab for Servers”, this section includes:

- **System Subtype.** Storage systems use the following subtypes:
 - **Storage.** A system that is identified as part of the storage infrastructure.
 - **SMI.** A system that was discovered through an SMI-S provider.
 - **Storage Essentials Managed.** A system that is managed by HP Storage Essentials.

Note:



If a system is managed by HP Storage Essentials, it does not show the **SMI** subtype.

- **Product Name.** The product name for the tape library, for example, a model number.
- **Product Vendor.** The tape library vendor.
- **Product Identifying Number.** A unique identifier for the tape library, for example, a serial number.
- **Product Version.** The tape library product version.
- **Firmware Version.** The installed firmware version.
- **Firmware Manufacturer.** The firmware manufacturer.

- **BIOS/FCode Version.** The installed BIOS/FCode version.
- **BIOS/FCode Manufacturer.** The BIOS/FCode manufacturer.
- **Management Proxies.** The servers that manage the selected tape library through a management protocol, such as WBEM.
- **Software Version.** The version of the software installed on this system.
- **Software Manufacturer.** The manufacturer of the software installed on this system.

Note:



Some vendors enter firmware details in the **Software Version** and **Software Manufacturer** fields instead of the **Firmware Version** and **Firmware Manufacturer** fields. These fields might display data about any software related to the system.

Ports

Note:



This section can be expanded or collapsed by clicking  and .

This section lists the tape library's Fibre Channel ports.

- **Element Name.** A user-friendly name for the port.
- **WWN.** The port's world wide name.
- **Port Type.** The port type. Refer to "Port Types" for additional information about port types.
- **Status.** The port's WBEM operational status. Refer to "WBEM Operational Status Types" for additional information about WBEM status.

Media Access Devices

Note:



This section can be expanded or collapsed by clicking  and .

This section lists the tape library's storage media, for example, data cartridges or disk drives.

- **Name.** The name of the storage media.

- **Status.** The media access device's WBEM operational status. Refer to “WBEM Operational Status Types” for additional information about WBEM status.
- **Firmware Version.** The installed firmware version.

Changer Devices

Note:



This section can be expanded or collapsed by clicking  and .

This section lists the tape library's changer devices, for example, the tape drive robotics.

- **Name.** The name of the changer device.
- **Status.** The changer device's WBEM operational status. Refer to “WBEM Operational Status Types” for additional information about WBEM status.
- **Firmware Version.** The installed firmware version.

Related Topics

- System Page
- Identity Tab for Servers
- WBEM Operational Status Types
- Port Types
- Data Collection

Port Types

HP Systems Insight Manager (HP SIM) displays port types for storage systems. If the values are supplied by a storage system's SMI-S provider, the port link technology and port type are displayed.

The possible port link technologies are **Unknown, Other, Ethernet, IB, FC, FDDI, ATM, Token Ring, Frame Relay, Infrared, BlueTooth,** and **Wireless LAN.**

The port type is displayed if it is one of the following:

- **N-Port.** A node port.
- **NL-Port.** A node port that supports Fibre Channel arbitrated loop (FC-AL),
- **E-Port** An expansion port that connects fabric elements (for example, FC switches).
- **F-Port.** A fabric (element) port.
- **FL-Port.** A fabric (element) port that supports FC-AL.
- **B-Port.** A bridge.
- **G-Port.** A generic port.

- **Other.** Any port type that does not fit the previously described categories.

Related Topics

- Identity Tab for a Tape Library
- Identity Tab for a Storage Switch
- Identity Tab for a Storage Host
- Identity Tab for a Storage Array

Tools & Links Tab

The system links that you can view depend on the Discovery configuration, the correct installation of agents and protocols, and the Polling Tasks that interrogate the system. The **Tools & Links** page includes:

- System Management Pages
- System Web Application Pages
- HP Systems Insight Manager Pages
- Storage Essentials Pages

Note:



In some cases, depending on the DNS configurations, you might need to use the IP address or a Fully Qualified DNS name to make the links work appropriately. Refer to “Configuring the System Link” for more information.

System Management Pages

This section includes the links that are provided by the HTTP Web Management on the system. These links are for system management and status. If the system does not have Insight Management Agent, this section is not displayed. Some of the available links include:

- **HP Version Control Agent**
- **HP Version Control Repository Manager**
- **HP Insight Management Agent**

System Web Application Pages

This section includes a list of Web applications hosted by the system. Some of the available links include:

- **VMware Management Interface**
- **Default Web Server**
- **HP SIM**

HP Systems Insight Manager Pages

This section contains links that are generated by HP Systems Insight Manager (HP SIM). Some of the available links include:

- The **Data Collection Report** link displays the data collection report for the system in a separate report results window.

Note:



The storage tables in HP SIM's Data Collection reports are not populated with data because HP SIM's SMI-S data collection is disabled.

-
- The **System Protocol Settings** link points to the **Protocol Settings**, where you can set the protocol settings for this individual system only.
 - The **Edit System Properties** link enables users with full-configuration-rights to re-configure some of the system properties for a single system through its system page. This link is not available if you do not have full-configuration-rights.

Refer to “Editing System Properties for Multiple Systems” for information on setting system properties for multiple systems.

- The **Suspend/Resume Monitoring** link enables you to set the timer for suspending monitoring. This allows a system to be excluded from the status polling, identification, data collection, and the automatic event handling features of HP SIM. The available suspend lengths include the pre-determined increments of 5 minutes, 15 minutes, 1 hour and 1 day. The suspend feature can be turned on indefinitely. This link is only available to users with full-configuration-rights.

Refer to “Suspending or Resuming System Monitoring for Multiple Systems” for information on suspending or resuming monitoring for multiple systems.

Storage Essentials Pages

This section is added when HP Storage Essentials is installed. Refer to your HP Storage Essentials documentation for details about the links that are added.

Related Procedures

- Editing System Properties for a Single System
- Suspending or Resuming System Monitoring for a Single System
- Editing System Properties for Multiple Systems
- Suspending or Resuming System Monitoring for Multiple Systems

Related Topic

- System Page
- Editing System Properties for a Single System
- Suspending or Resuming System Monitoring for a Single System

Version Control

The HP Version Control Repository Manager (VCRM) and HP Version Control Agent (VCA) are Web-enabled HP Insight Management Agents. HP Systems Insight Manager uses these Insight Management Agent and others to facilitate Software Update and tasks related to it.

In general, HP Insight Management Agent 4.0 and later are Web enabled, and they provide in-depth subsystem status and fault information on servers, workstations, desktops, and portables, communicating directly with HP SIM when they are launched. Web-enabled agents are accessible directly through a browser or through HP SIM.

HP SIM provides the following version control tools:

- **Install Software and Firmware.** Select **Deploy->Deploy Drivers, Firmware and Agents->Install Software and Firmware.**
- **Initial ProLiant Support Pack Install.** Select **Deploy->Deploy Drivers, Firmware and Agents->Initial ProLiant Support Pack Install.**

Related Procedures

- Installing Software and Firmware
- Initial ProLiant Support Pack Install

Related Topics

- Creating a Replicate Agent Settings Task
- About the Version Control Agent
- About the Version Control Repository Manager
- About Integration
- About Multiple System Management
- About Software Repositories

About the Version Control Agent

The HP Version Control Agent (VCA) is an HP Insight Management Agent that is installed on a system to enable you to view the HP software and firmware that is installed on that system. The VCA can be configured to point to a repository being managed by the HP Version Control Repository Manager (VCRM), allowing easy version comparison and software updates from the repository to the system on which the VCA is installed.

The VCA provides version control and system update capabilities for a single HP system. The VCA determines system software status by comparing each component installed on the local system with the set of individual components or a specified ProLiant or Integrity Support Pack listed in the VCRM. You can also update individual components or an entire ProLiant or Integrity Support Pack by clicking the install icon located next to the system software status icon.

The VCRM and the VCA are integrated with the System Management Homepage (SMH), which is the standard single-server management tool in the ProLiant Essentials Foundation Pack. HP Systems Insight Manager (HP SIM), also part of the ProLiant Essentials Foundation Pack, uses the VCRM and VCA to facilitate software versioning, update, and tasks related to it.

The VCA is available for Windows and Linux operating systems. The VCA is an integrated part of the System Management Homepage that is designed to display the available software inventory of the system on which it is installed. The VCA also allows the installation, comparison, and update of system software from a repository that is managed by a VCRM.

Users with administrator or operator privileges can access the VCA to maintain the software inventory of the system manually. The installation of components and configuration activities are

logged to a log file at the system. The VCA logs activities, such as software installations. However, installations done outside the VCA do not appear in this log.

The VCA enables you to view the software installed on selected HP equipment, the available updates, and whether the installed software is compliant with the latest updates found in the selected repository. In addition, you can add or update HP software on the system remotely, using the browser interface of the VCA.

You can use the Replicate Agent Settings feature in HP SIM to update multiple servers with VCA settings. For more information regarding the **Replicate Agent Settings** feature, refer to the online HP SIM help system.

The VCA permits the following tasks:

- Viewing the currently installed software
- Selecting a VCRM as a reference point for obtaining software updates
- Selecting a ProLiant or Integrity Support Pack as a managed baseline.
- Viewing the details associated with a ProLiant or Integrity Support Pack or individual software component that is in the version control repository
- Installing a ProLiant or Integrity Support Pack or individual software component from the version control repository
- Printing the installed software inventory and software status
- Managing the VCA log

In addition to maintaining the software inventory of the system, the VCA integrates with HP SIM. This integration enables administrators to take advantage of the Software Update capabilities of the agent

Additional Resources

For additional resources, go to <http://www.hp.com/servers/manage>.

Related Procedures

- Installing Software and Firmware
- Initial ProLiant Support Pack Install

Related Topics

- Version Control
- About Integration
- About Multiple System Management
- About Software Repositories

About the Version Control Repository Manager

The HP Version Control Repository Manager (VCRM) is an HP Insight Management Agent that manages a directory of HP software and firmware components. The VCRM can be used without the HP Version Control Agent (VCA) to provide a listing of available software and firmware to load on the local machine. The VCRM is part of the ProLiant Essentials Foundation Pack.

The VCRM is designed to be used in a one-to-many configuration with a VCA installed on each managed HP system to manage installed HP software and firmware. In conjunction with HP Systems Insight Manager (HP SIM), the VCRM and VCAs provide enterprise-wide management of HP

software and firmware on HP ProLiant and Integrity systems. Alone, the VCRM can be used to catalog and manage a repository of ProLiant and Integrity Support Packs, and individual software and firmware from HP for HP ProLiant and Integrity systems.

Note:



Although it is possible to install a HP ProLiant and Integrity Support Pack or component to the local machine using the VCRM, you cannot install the software on remote servers unless the VCA has been installed on the remote server and the install is initiated using the VCA.

The VCRM permits the following tasks:

- Viewing the contents of the repository, such as ProLiant Support Packs or component details
- Configuring Automatic Update to proactively deliver new ProLiant software from HP as it is made available
- Uploading a support pack to the repository from a CD or other accessible media using the **Upload a Support Pack** feature
- Creating HP ProLiant and HP Integrity Support Packs
- Deleting HP ProLiant and HP Integrity Support Packs and components
- Copying HP ProLiant and HP Integrity Support Packs and components to another repository
- Configuring components in the repository that are flagged as requiring configuration
- Updating from HP.com now
- Rescanning the repository and rebuilding the catalog
- Managing the log
- Installing selected components at the local (browser client) system

Additional Resources

For additional resources, go to <http://www.hp.com/servers/manage>.

Related Procedures

- Installing Software and Firmware
- Initial ProLiant Support Pack Install

Related Topics

- Version Control
- About Integration
- About Multiple System Management
- About Software Repositories

About Integration

For software versioning and updating, HP Systems Insight Manager (HP SIM) relies on the VCRM and the VCA. By using these applications, HP SIM provides a single view of the software status for all managed ProLiant or Integrity servers, plus the capability to update software and firmware on those servers through its powerful query and task features. Updates can be scheduled and applied to specific sets of servers based on predetermined criteria, including applying updates only to those systems that require an update.

To take full advantage of the software update capabilities of HP SIM, ensure that:

- Every managed target server on the network has the VCA installed and is configured to use a repository
- Every repository that is to be used has the VCRM installed
- You can optionally use the automatic update feature of the VCRM to update all repositories with the latest software from HP automatically

Related Procedures

- Installing Software and Firmware
- Initial ProLiant Support Pack Install

Related Topics

- Version Control
- About the Version Control Agent
- About the Version Control Repository Manager

About Software Repositories

The practice of updating ProLiant Support Packs and components using VCRM from a single or multiple repositories saves time and is key to standardizing software maintenance and update procedures on distributed systems.

For maximum manageability and flexibility across operating system platforms, each repository that is created should conform to the following conditions:

- Located on a local drive with write access
- Updated automatically by the VCRM

When a repository has been created, the repository must be populated with ProLiant Support Packs and components before being updated on the target HP systems. Although it is optional, the easiest and most efficient way to update a repository is by using the Automatic Update feature of the VCRM. The Automatic Update feature of the VCRM enables you to schedule an automatic population of the repository. However, the repository can be updated in any, or combination of any, of the following ways:

- The Automatic Update feature of the VCRM
- The Upload ProLiant Support Pack feature of the VCRM, which enables users to easily copy ProLiant Support Packs from a SmartStart CD or other accessible media
- Manually downloading the software into the repository from <http://www.hp.com>

Related Procedures

- Installing Software and Firmware
- Initial ProLiant Support Pack Install

Related Topics

- Version Control
- About Integration
- About the Version Control Agent
- About the Version Control Repository Manager

About Multiple System Management

The Software Update capabilities of HP Systems Insight Manager (HP SIM) includes the following features:

- **Initial ProLiant Support Pack Install.** This feature enables you to install the latest desired ProLiant Support Pack from the specified VCRM. It is for use only on target systems **not** running the HP Version Control Agent. This feature is only available on Windows systems. If the VCA is already installed on managed systems, you can use the Install Software and Firmware task to update.
- **Install Software and Firmware.** This feature enables you to automatically update ProLiant Support Packs and components onto HP systems managed by HP SIM. The target systems must have the VCA installed.
- **Searching by systems with Software/Firmware.** This search criterion enables you to quickly create and display a list of systems with specific software or firmware versions. For example, a user with full-configuration-rights might want to locate and display all HP systems with HP Insight Management Agent less than a defined version. The search can then be used with the Install Software and Firmware Task to update the systems to the current version of Insight Management Agent.
- **Software Version Status Polling.** Software and firmware upgrade status are retrieved from the VCA on target systems. Software and firmware inventory is also retrieved from those systems during this task.
- **Replicate Agent Settings.** This feature allows HP SIM to retrieve Web Agent configuration settings from a source device and distribute that configuration to one or more target devices through their Web Agents.

All of these system software management enhancements rely on the tight integration of HP SIM with the HP Version Control Repository Manager and the HP Version Control Agent.

Related Procedures

- Installing Software and Firmware
- Initial ProLiant Support Pack Install

Related Topics

- Version Control
- About Integration
- About Software Repositories
- Replicating Trusted Certificates

Accessing the Version Control Agent

Access the HP Version Control Agent (VCA) graphical user interface (GUI) from any network client using a Web browser. For information about which browsers are supported, refer to the HP Version Control Installation Guide at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

Important:



If an HP Version Control Repository Manager (VCRM) has not been configured, only the Software and Firmware Inventory of items currently installed on the system are displayed on the **Home** page. The VCA settings must be configured for full functionality.

Important:



For Windows operating systems, you must install the HP Insight Management Agent 5.40 or later to obtain any inventory data. For Linux operating systems, you must install HP Server Management Application and Agents (hpsasm RPM) 7.00 or later to obtain any inventory data. HP recommends installing the current version that is in the same HP ProLiant and Integrity Support Pack as the VCA.

Note:



If the Insight Management Agents are not installed, software inventory cannot be collected by the VCA. The VCA can still be used to install software, however.

Note:



Login accounts which have Administrator or Operator privileges defined in the System Management Homepage can access all features of the VCA.

Logging into the VCA

To login to the VCA:

1. To access the VCA with access to all available features, you must login to the System Management Homepage with **administrator** or **operator** level access.
2. Navigate to **https://hostname:2381**. The **Login** page appears if **Anonymous Access** is disabled. If **Anonymous Access** is enabled, the **System Management Homepage** page appears.

3. After you have logged in, you can browse directly to the VCA by entering **https://hostname:2381/vcagent** in the browser address field, or you can open it in a new browser window by clicking the HP Version Control Agent link from the System Management Homepage under **Integrated Agents**, or in the **Version Control** status box on the **Home** tab. The **VCA** page appears.

Related Procedure

- Accessing the Version Control Repository Manager

Related Topics

- System Page
- System Management Homepage

Accessing the Version Control Repository Manager

There are two ways to access the HP Version Control Repository Manager including:

- Accessing VCRM from HP Systems Insight Manager (HP SIM)
- Accessing VCRM directly

Accessing VCRM from HP SIM

To access the VCRM from HP SIM:

1. Select **Tools->System Information->System Management Homepage**.
2. Select the target system and click **Run Now**. Refer to “Creating a Task” for more information. The System Management Homepage appears.
3. From the **Verify Target Systems** page, click **Run Now**.
4. From System Management Homepage, click the **HP Version Control Repository Manager** link. The **VCRM Home** page appears.

or

From System Management Homepage, select **Tools** and click the **HP Version Control Repository Manager** link.

Accessing VCRM In-Place

Navigate to **http://hostname:2381/vcrepository** on the system that has the VCRM installed. The **VCRM Home** page appears.

Related Procedure

- Accessing the Version Control Agent

Related Topics

- System Page

- System Management Homepage

Version Control Status Icons

Note:



Click a **Software Status** icon to access the HP Version Control Agent (VCA). If the VCA cannot be accessed, help displays describing how to configure the VCA or trust relationship on that system.

Note:



There is a **Software Status** icon for every server except HP-UX.

Version Control Status

The status is based on comparing the installed versions against versions in the repository.

Icon	Status
	<p>There are different reasons why an Unknown status icon might display:</p> <ul style="list-style-type: none"> ● The VCA does not have a HP Version Control Repository Manager (VCRM) configured. ● The configured VCRM is not reachable or does not respond to HTTP requests, for example, the system or service is down or the password has been changed. ● A VCA cannot be detected on the system or cannot communicate with the VCA.

Status Values When no Reference Support Pack is Set

Note: The status is that of the latest version of the component in the configured repository.

Icon	Status
	This update contains critical bug fixes. HP requires that you apply this update at your earliest convenience.

Icon	Status
	The repository contains a version of this component that might contain bug fixes or new hardware support. HP recommends that you review information about this version and apply this update appropriately.
	The installed software versions are the same or newer than the latest versions available at the VCRM.

Status Values When a Reference Support Pack is Set but the Exact Match Setting is Not Selected

Icon	Status
	This update contains critical bug fixes. HP requires that you apply this update at your earliest convenience.
	This update might contain bug fixes or new hardware support. HP recommends that you review information about this version and apply this update appropriately.
	The installed software versions are the same or newer than the versions in the Reference Support Pack.
	The Reference Support Pack configured at the VCA is no longer valid at the configured VCRM.

Status Values When a Reference Support Pack is Set and the Exact Match is Selected

Icon	Status
	The installed version does not match the version of the same item in the Reference Support Pack, and the VCA settings specify that an exact match is expected.
	The installed software versions are the same or newer than the versions in the Reference Support Pack.
	The Reference Support Pack configured at the VCA is no longer valid at the configured VCRM.

When the overall software status indicates that an item is not current, identify the software or firmware items that have available updates, read the item descriptions, and determine whether the update is appropriate for the server.

In the event a repository has been configured and a Reference Support Pack has not, the status is based on a comparison between the installed software or firmware versions and the newest components available from the configured repository.

In the event a repository and Reference Support Pack have been configured, the status is based on a comparison between the installed software or firmware versions and the software or firmware versions in the Reference Support Pack.

Related Procedures

- Installing Software and Firmware
- Initial ProLiant Support Pack Install

Related Topics

- About the Version Control Agent
- About the Version Control Repository Manager

Installing Software and Firmware

To update managed servers with the most current software, HP SIM provides software update capabilities that use the HP Version Control Agent (VCA) and HP Version Control Repository Manager (VCRM).

Automated software updates through HP SIM have the following restrictions:

- Updates can be performed only on ProLiant servers that have the VCA installed and trust the HP SIM server. The Install Software and Firmware feature can only be used with third-party systems running the VCA.

Note: Refer to “Trusted Certificates” for information regarding trust relationships. After the trust relationship is established, click **Last Update** to update the display to trusted.

- Updates require ProLiant Support Pack or components, version 5.3 or later. The Install Software and Firmware feature does not support third-party software.
- Updates are supported on Linux, Windows NT 4.0, Windows 2000, and Windows Server 2003 operating systems.
- Updates cannot be made on the CMS

To install software and firmware:

1. Select **Deploy->Deploy Drivers, Firmware and Agents->Install Software and Firmware**. The **Install Software and Firmware** page appears.
2. Select target systems. Refer to “Creating a Task” for more information.
3. Click **Next**.
4. Under **Select Items to Install**, select the repository from which to retrieve the catalog.
Note: This section only displays systems that are authorized by the current user name.
5. Under **Contents of selected version control repository**, click the  icon to drill down and view the contents of the Version Control Repository that you selected.

Note: To expand the tree to display all contents, click the  icon located in the upper left corner of the **Contents of selected Version Control Repository** section. Click the  icon to collapse the listings.

Select the components you want to install.

6. Click **Next**.

The **Select Install Options** section appears.

7. The items are installed in the order in which they are listed. To reorder the items,
 - a. Select the item to reorder, and click **Move Up** to advance the item up.
or
 - b. Click **Move Down** to move the item down.
8. Select **Force downgrade or re-install if necessary** if you are installing software that is older than or the same as the version currently installed. This option is disabled by default.
9. Select **Bring systems to full power before install** if you want to bring systems to full power before the installation. If this option is not selected, the installation is attempted and might fail because the system was not running at full power.

Note: The targeted system must support Magic Pocket technology to be brought to full power.

If selected, the target systems are brought to full power before the install is selected.

10. By default, **Reboot systems if necessary after successful install** is selected. You can deselect this option if you do not want to reboot after the installation. However, the successful task status indicates that a reboot is required to complete the update.
11. Click **Schedule** to configure a time for the update to occur. Refer to “Scheduling a Task” for more information on scheduling the task. Click **Previous** to return to the previous screen, or click **Run Now** to immediately install the software.

If you click **Schedule**, the **Schedule Task** section appears.

Firmware Deployment to Switches

When deploying firmware to switches, verify that:

- When updated HP switch firmware, only switch devices and a single switch firmware component are selected.
- That the switch firmware image version always matches the switch firmware boot image.
- Some of the older switch components do not generate a log file. The switch update status can be found by running the ProLiant Interconnect Switch Upgrade tool. This tool is installed automatically as part of an Install Software/Firmware Task to a switch device.

Related Procedures

- Scheduling a Task

- Task Results List

Related Topics

- Version Control
- Replicating Trusted Certificates

Initial ProLiant Support Pack Install

The Initial ProLiant Support Pack Install process enables you to install a ProLiant Support Pack to a Windows system because you do not have any HP Insight Management Agents, especially HP Version Control Agent, installed. This process also configures the systems to use the trust certificate from the HP Systems Insight Manager (HP SIM) and the setting to use the desired HP Version Control Repository Manager (VCRM).

Note:



The Initial ProLiant Support Pack Install feature is only supported on Windows central management servers.

The target system must be a Windows system. The Install Software and Firmware feature in HP SIM requires that the HP Version Control Repository Manager be installed on servers containing a repository. Installing the VCRM is not part of this procedure. For more information regarding installing the VCRM, refer to the HP Version Control Installation Guide at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

Note:



You must have Windows administrator privileges on target systems to install a ProLiant Support Pack.

Note:



The Install Software and Firmware and VCA tasks are only available to systems running a properly configured VCA. Running the Initial ProLiant Support Pack task enables you to install the VCA quickly and easily.

Note:



For more information regarding ProLiant Support Packs, refer to the *HP ProLiant Support Pack and Deployment Utilities User Guide* at <http://h18013.www1.hp.com/manage/psp.html>.

To install a ProLiant Support Pack:

1. Select **Deploy->Deploy Drivers, Firmware and Agents->Initial ProLiant Support Pack Install**. The **Initial ProLiant Support Pack Install** page appears.
2. Select the target systems. Refer to “Managing with Tasks” for more information.
3. Click **Next**.
4. From the **Enter Windows login credentials** page:
 - a. In the **User name** field, enter the Windows administrator user name for the target system.
 - b. In the **Password** field, enter the administrator password for the Windows user name entered above.
 - c. In the **Password (Verify)** field, reenter the Windows administrator password exactly as it was entered in the **Password** field.
 - d. In the **Domain** field, enter the Windows domain.

Note: This field can be left blank if the system is not part of a domain.

5. Click **Next**. The **Select a Windows Support Pack** page appears.
6. Under **Select a Version Control Repository**, select a source repository system from which to retrieve the catalog.

The following fields display:

- **Name**. This field displays the name of the system.
- **Status**. This field displays the status of the system.
- **Product Name**. This field displays the name of the product.
- **Trusted?**. This field indicates whether the system trust relationship has been configured. To configure a trust relationship, click **configure**. Refer to “Trusted Certificates” for more information.

Note: This section displays systems that are authorized by the current user name. If the current user is not authorized to view the systems, a message appears, indicating that the user does not have authorization rights on the system.

7. Under **Select a Support Pack to Install**, select a support pack to install. Click the  icon to drill down and view the contents of the Version Control Repository that you selected.

Note: To expand the **System Software Baseline** to display all contents, click the  icon located in the upper left corner of the **Select a Support Pack to Install** section. Click the  icon to collapse the listings.

8. Select **Install and initialize SSH (Secure Shell)** if you want to install and configure OpenSSH on the target systems. This option is disabled by default.
9. (Optional) Select **Force downgrade or re-install the same version** if you are installing a ProLiant Support Pack that is older than or the same as the version currently installed. This option is disabled by default.
10. By default, **Reboot systems if necessary after successful install** is selected. You can deselect this option if you do not want to reboot after the installation. However, the system must be rebooted for the new ProLiant Support Pack to be available.
11. Click **Next**. The **Configure Support Pack** page appears.

- If you select a ProLiant Support Pack 7.10, **Configure a Support Pack** appears. For example:

Note: If you select a ProLiant Support Pack that is earlier than 7.10, the following example varies.

To configure the 7.10 support pack:

- a. Click **Configure Support Pack** to set up the HP Version Control Agent in the selected Support Pack. The **VCA Setup** page appears.

Note: If the VCA has already been configured, you can omit this step.
- b. In the **Computer Name** field, enter the name of the system where the VCRM is installed.
- c. In the **Administrator Password** field, enter the password associated with the login name specified.
- d. Click **Save** to save your settings. Click **Cancel** to discard your settings and close the **VCA Setup** page.
- e. Click **Next**. The **Download Support Pack** page appears.
- f. After the support pack is downloaded, click **Schedule** to create a scheduled task for the Initial ProLiant Support Pack Install to run or click **Run Now** to run the task immediately.

If you select a ProLiant Support Pack 7.20 or later, the following options display.

- Click **Configure System Management Homepage** to setup the Support Pack to establish a trust relationship with System Management Homepage when it is installed on target systems. The **Welcome to the Configuration Wizard for the HP System Management Homepage Component** page appears.

Note: If the Support Pack has already been configured, you can skip this step.

Note: Refer to “Trusted Certificates” for more information on setting up a trust relationship. After the trust relationship is established, click **Last Update** to update the status to trusted.

To configure the System Management Homepage:

- a. From the **Welcome to the Configuration Wizard for the HP System Management Homepage Component** page, click **Next**. The **Operating Systems Groups** page appears.
- b. In the **Group Name** field, enter the name of an operating system group that you want to assign. For example, *vcadmin*.
- c. In the **Operating Level** field, select the appropriate level for the new group from the dropdown list.

Note: The default **Administrators Groups** always have administrative access.

- d. Click **Add** to assign the group. The new group appears under the operating system group which it was assigned.

Note: You can add up to five entries per operating system group.

- e. Click **Next**. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.
- f. **Local** and **Anonymous** access enables you to select the appropriate settings to include:

- Anonymous Access.** Anonymous Access is disabled by default. Enabling **Anonymous Access** enables a user to access the System Management Homepage (SMH) without logging in. Select this option to allow anonymous access.

Caution: HP does not recommend the use of anonymous access.

- Local Access.** Local Access is disabled by default. Enabling it means you can locally gain access to the System Management Homepage without being challenged for authentication. This means that any user with access to the local console is granted full access if **Administrator** is selected. If **Anonymous** is selected, any local user has access limited to unsecured pages without being challenged for a username and password. Select this option to allow local access.

Caution: HP does not recommend the use of local access unless your management server software enables it.

- g. Click **Next**. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.
- h. The **Trust Mode** options enable you to select the security required by your system. There are some situations that require a higher level of security than others. Therefore, you are given the following security options:
 - Trust by Certificate.** Sets the System Management Homepage (SMH) to accept configuration changes only from HP SIM servers with trusted certificates. This mode requires the submitted server to provide authentication by means of certificates. This mode is the strongest method of security since it requires certificate data and verifies the digital signature before allowing access. If you

do not want to enable any remote configuration changes, leave **Trust by Certificate** selected, and leave the list of trusted systems empty by avoiding importing any certificates.

Note:



HP strongly recommends using this option as it is more secure.

To trust by certificate:

1. Select **Trust by Certificate** and click **Next**.
 2. In the **Certificate Name** field, click **Browse** to select the certificate file. After the certificate file is selected, the certificate data is displayed on the screen.
 3. Click **Add**. The certificate appears under **Certificate Files**. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.
 4. Click **Next**. The **IP Binding** page appears.
- Trust by Name.** Sets the System Management Homepage to accept certain configuration changes only from servers with the HP SIM names designated in the **Trust By Name** field. The **Trust By Name** option is easy to configure. For example, you might use the trust by name option if you have a secure network with two separate groups of administrators in two separate divisions. It prevents one group from installing software to the wrong system. This option verifies only the HP SIM server name submitted.

Note:



HP strongly recommends using the **Trust by Certificate** option as the other options are less secure.

The server name option must meet the following criteria:

- Each server name must be less than 64 characters
- The overall length of the server name list is 1,024 characters
- Special characters should not be included as part of the *server name*: ~ ' ! @ # \$ % ^ & * () + = \ " : ' < > ? , |
- Semicolons are used to separate *server names*

To trust by name:

1. Select **Trust by Name** and click **Next**.
 2. In the **Trusted Server Name** field, enter the server name to be trusted.
 3. Click **Add**. The trusted system name appears under the **Trusted Servers** list. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.
 4. Click **Next**. The **IP Binding** page appears.
- Trust All.** Sets the System Management Homepage to accept certain configuration changes from any system.

Note:



HP strongly recommends using the **Trust by Certificate** option as the other options are less secure.

To trust all servers:

1. Select **Trust All**. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.
 2. Click **Next**. The **IP Binding** page appears.
- i. IP Binding specifies from which IP addresses the System Management Homepage (SMH) accepts requests from and provides control over which nets and subnets requests are processed.

Administrators can configure the System Management Homepage to only bind to addresses specified in the **IP Binding** page. A maximum of five subnet IP addresses and netmasks can be defined.

An IP address on the server is bound if it matches one of the entered IP Binding addresses after the mask is applied.

Note:



The System Management Homepage always binds to 127.0.0.1. If IP Binding is enabled and no subnet/mask pairs are configured, then the System Management Homepage is only available to 127.0.0.1. If IP Binding is not enabled, you bind to all addresses.

To configure IP Binding:

1. Select **IP Binding**. The **IP Binding** page appears.
 2. Enter the IP address.
 3. Enter the Netmask.
 4. Click **Add**. The IP binding configuration is saved and appears under the **IP Binding List**.
 5. Click **Next**. The **IP Restricted Login** page appears.
- j. The IP Restricted Login enables the System Management Homepage (SMH) to restrict log-in access based on the IP address of a system.

You can set address restriction at installation time or by it can be set by administrators from the **IP Restricted Login** page

- If an IP address is excluded, it is excluded even if it is also listed in the included box.
- If there are IP addresses in the inclusion list, then only those IP addresses are allowed log-in access with the exception of *localhost*.
- If no IP addresses are in the inclusion list, then log-in access is allowed to any IP addresses not in the exclusion list.

To include or exclude IP addresses:

1. In the **From** field, enter the IP addresses to include or exclude. You can enter an IP address range to be included or excluded by entering a beginning IP address in the **From** field and an ending IP address in the **To** field.
 2. From the **Type** field, select **Include** or **Exclude**.
 3. Click **Add** to add the IP address or IP address range to the **Inclusion List** or **Exclusion List** below.
 4. Click **Save**. The **HP System Management Homepage Login** page for the System Management Homepage system appears. For more information about System Management Homepage, refer to the System Management Homepage Online Help at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.
- Click **Configure VCA** to set up the HP Version Control Agent in the selected Support Pack.

Note: If the VCA has already been configured, you can skip this step.

To configure the VCA:

- a. In the **Computer Name** field, enter the name of the system where the VCRM is installed.
- b. In the **Login Account** field, enter the login name used to connect to the VCRM on the system specified.

- c. In the **Login Password** field, enter the password associated with the login name specified.
 - d. Click **Save** to save your settings. Click **Cancel** to discard your settings and close the **VCA Setup** page.
 - e. Click **Next**.
12. Back in HP SIM, click **Next** to start the ProLiant Support Pack download. The **Download Support Pack** page appears.
 13. After the support pack is downloaded, click **Schedule** to create a scheduled task for the Initial ProLiant Support Pack Install to run or click **Run Now** to run the task immediately.

Related Procedure

- Installing Software and Firmware
- Setting Up Managed Systems

Related Topic

- About the Version Control Repository Manager

Virtual Machine Management Pack

HP ProLiant Essentials Virtual Machine Management Pack (VMM) provides central management and control for virtual machines of type Microsoft's Virtual Server and VMware's GSX or ESX. Using VMM, all virtual machines and Virtual Machine (VM) hosts can be managed from the HP Systems Insight Manager (HP SIM) console.

VMM is ideal in the following environments:

When implementing one of the following projects (or others) that involve server virtualization:

- Server Consolidation projects. VMM reduces server sprawl using virtualization technology to host several servers on one physical server
- Disaster Recovery projects. VMM helps maintain disaster recovery site without using same number of physical servers
- Test and Development projects. VMM uses VMs to quickly provision and scale test machines and rapidly transition to newer projects
- Client Consolidation projects. VMM hosts several clients on high capacity servers, reducing the manageability burden associated with stand alone clients

When you are looking to:

- Looking to use existing employees, processes, and tools to manage VMs in addition to physical servers

- Looking for common management irrespective of virtualization layer (VMware ESX/GSX or Microsoft Virtual Server)
- Looking for easy and rapid migrations between physical and virtual platforms (physical to virtual (P2V), virtual to physical (V2P), and virtual to virtual (V2V))

Workload management and legacy environments.

- Workload Management. Leverage ability to easily move VMs from server to server to manage server workloads
- Extend life of legacy environments. Take advantage of ability to run legacy applications in a VM that removes dependence on specific hardware

The **Virtual Machine Management Pack** displays a tree view of the VM hosts and VM guests in the left pane of the HP SIM console. After selecting a system in the left pane tree, information for the system selected is displayed in the right pane.

VMM consists of two major installed components: the VMM service and the VMM agent. The VMM service must be installed on the HP SIM central management server (CMS) on a supported Windows platform. The VMM service:

- Provides the user interface
- Interfaces with HP SIM
- Directs the VMM agent, installed on VMware ESX and Windows VM hosts, to perform VM management activities on licensed VM hosts.

A VMM agent on VM hosts can be directed to perform VM control operations (start, stop, pause, and so on) and copy and move VMs among VM hosts from the HP SIM console.

HP SIM relies on VMM to identify VM hosts during the Identification process. Once HP SIM has identified a system as a server, it determines if the system is a VM host. If VMM indicates to HP SIM that the system is a VM host, it is displayed as such in the console, and the VMM functionality is enabled for that system..

Related Procedures

- Deploying the VMM Agent
- Registering VMM
- Unregistering VMM
- Upgrading VMM

Related Topic

- VM Status Types

Deploying the VMM Agent

This tool is used to deploy the HP ProLiant Essentials Virtual Machine Management Pack agent on the target Virtual Machine (VM) hosts. Multiple VM hosts can be selected to deploy the agent. This agent enables HP Systems Insight Manager (HP SIM) to identify, through the HP ProLiant Essentials Virtual Machine Management Pack server, whether the server is a VM host.

You must have limited or full-configuration-rights to perform this procedure.

Note:



OpenSSH must be installed on Windows servers before the VMM agent can be deployed from the central management server (CMS). Refer to “Installing OpenSSH” for information on installing OpenSSH.

To deploy the Windows agent to Windows VM hosts:

1. Select **Deploy>Drivers, Firmware and Agents>Install VMM Agent>Windows**.
2. Select the target Windows VM hosts by selecting the checkbox next to the appropriate systems.
3. Click **Apply**.
4. (Optional) Click **Add Targets** to add additional targets, or click **Remove Targets** to remove targets, and then click **Next**.
5. Click **Run Now** to start the deployment immediately, or click **Schedule** to deploy the VMM agent at a later time.
6. View the task results in the HP SIM task logs.

To deploy the Linux agent to Linux VM hosts:

1. Select **Deploy>Drivers, Firmware and Agents>Install VMM Agent>Linux**.
2. Select target VM hosts by selecting the checkbox next to the appropriate systems.
3. Click **Apply**.
4. (Optional) Click **Add Targets** to add additional targets, or click **Remove Targets** to remove targets, and then click **Next**.
5. Click **Run Now** to start the deployment immediately, or click **Schedule** to deploy the VMM agent at a later time.
6. View the task results in the HP SIM task logs.

Note:



The VMware ESX Server host uses the VMM Linux agent.

Related Topics

- Virtual Machine Management Pack
- VM Status Types

Registering VMM

This tool establishes communication between the Virtual Machine (VM) Host and HP ProLiant Essentials Virtual Machine Management Pack console. When registration is complete, the VM host status is displayed in the VM column.

To register a VM host:

1. From the **All Systems** page, select the checkbox next to the VM host.
2. Select **Configure**->**Virtual Machine Host Registration**->**Register VM Host**.
3. Verify the target VM host, and click **Next**.
4. Click **Run Now** to register the host immediately.

Related Procedure

- Unregistering VMM

Related Topics

- Virtual Machine Management Pack
- VM Status Types

Unregistering VMM

This tool terminates communication between the virtual machine host and HP ProLiant Essentials Virtual Machine Management Pack. The HP ProLiant Essentials Virtual Machine Management Pack can no longer communicate with unregistered Virtual Machine (VM) hosts.

To unregister a VM host:

1. From the **All Systems** page, select the checkbox next to the VM host.
2. Select **Configure**->**Virtual Machine Host Registration**->**Unregister VM Host**.
3. Verify the target VM host, and click **Next**.
4. Click **Run Now** to unregister the host immediately.

Related Procedure

- Registering VMM

Related Topics

- Virtual Machine Management Pack
- VM Status Types

Upgrading VMM

This tool is used to upgrade the HP ProLiant Essentials Virtual Machine Management Pack (VMM) agent from a previous version to the current version for all of the previously managed Virtual Machine (VM) hosts without user interaction. This menu appears when the installation has detected that a previous version of VMM exists. If an upgrade is required, the **Tasks Results** page appears. Click **Schedule** to schedule when to run the upgrade, or click **Run Now** to run the upgrade immediately.

Related Topics

- Virtual Machine Management Pack
- VM Status Types

VM Status Types

In HP Systems Insight Manager (HP SIM), a Virtual Machine (VM) host has one of the following status types:

Icon	Status
	The VM host is licensed and is currently communicating with VMM
	VM host is licensed for but is not currently communicating with VMM
	The VMM agent is installed on the server, but the server is not a VM host
	The VMM agent is installed on the VM host, but the host is not licensed
No icon	The VMM agent is not installed on this server

A VM guest has one of the following status types:

Icon	Status
	The VM guest is associated with a licensed VM host, and the guest is started
	VM host is licensed for but is not currently communicating with VMM
	The VM guest is associated with a licensed VM host, but the host is not communicating with VMM
	The VM guest is in a state requiring user attention
	The VM guest is associated with a licensed VM host, but the guest is not started
	The VM guest is not associated with a licensed VM host

Click any of these links in HP SIM to display additional information for the system.

Related Topic

- System Table View Page

WBEM Based Tools

Several WBEM-based tools are available in HP Systems Insight Manager (HP SIM), including:

- Properties pages
- System Fault Management

Note: If System Fault Management is not installed, HP SIM cannot recognize or see WBEM indications.

- WBEM Providers

Related Topics

- Property Pages
- System Fault Management Overview
- WBEM Providers Overview

Property Pages

The Web-Based Enterprise Management (WBEM) name and password pairs entered under **Options>Protocol Settings>Global Protocol Settings** also control the amount of data displayed on the **Property** pages. If the root name and password pair is not available, many of the properties are omitted because the target system providers require root access. The **Property** pages are used to view WBEM properties on remote target systems (HP-UX, HP-UX IPF, Linux IPF, Linux IA32, Windows, and Dec Alpha) and can be accessed in two ways:

- From the **System Page** on the **Identity** tab, click **Properties**. The **Property** pages display for the target system.
- Select **Tools>System Information>Properties**. Select the target system from here and click **Run now**. The **Property** pages display for the target system.

The **Property** pages open in a new window if launched from the **Systems Page** or from the **Tools** menu. The **Property** pages include three tabs:

- **Identity**. Displays WBEM properties that help describe the target system on the network. These properties can include such physical aspects as location, local time, operating system characteristics, and owner information.
- **Status**. Displays WBEM properties that help determine the status of the system. At a minimum, you can determine the memory status and process status. Depending on the target system installation of WBEM, you might be able to determine status on all of the major computer subsystems. A status icon for each component appears next to each of the status properties. Refer to “System Status Types” for more information on the hardware status icons that can be displayed.

- **Configuration.** Displays an inventory of the target system based on WBEM properties. At a minimum, this inventory includes operating system information, but it might also include information on CPUs, disk drives, file systems, motherboards, software installations, and networks.

Note:



The date and time displayed on the **Property** pages indicates the time on the target system.

System Fault Management Overview

System Fault Management is a suite of advanced hardware fault technologies that protects hardware against failures and reports predictive information and corrective action events. System Fault Management is available for HP 9000 systems running Version 2 Update 2, and Integrity servers running HP-UX 11i version 2 Update 2.

System Fault Management integrates into HP Systems Insight Manager (HP SIM) using industry-standard Web-Based Enterprise Management (WBEM) instrumentation.

Integration among standards-compliant system management applications, as with HP SIM, provides a holistic and comprehensive view of HP 9000 systems' and HP Integrity server's wellbeing.

System Fault Management uses industry-standard Desktop Management Taskforce (DMTF) WBEM to provide advanced system level monitoring capabilities to protect hardware against failures that could interrupt system operation.

In addition, System Fault Management allows for configuration of notification thresholds for reporting predictive information and corrective action events. Configurable thresholds enable system administrators to customize notifications to match the desired availability service level.

System Fault Management includes providers to gather and model information and deliver it to the network management application through an industry standard interface (that is, using CIM specifications, through XML over HTTP).

The CPU Instance Provider gathers information about the central processors of an HP 9000 server.

The Memory Instance Provider gathers information about the memory configuration of an HP 9000 server.

The EMS Wrapper Provider translates hardware events from Event Monitoring System (EMS) hardware monitors into a form that is compatible with WBEM.

System Fault Management is available in HP SIM by selecting a system with System Fault Management installed and then select **Tools->System Information->System Page**.

Go to <http://www.hp.com/products1/unix/operating/SysFaultMgmt.html> for additional information about System Fault Management.

WBEM Providers Overview

HP WBEM Management Providers allow you to remotely monitor system configuration and status. The Management Providers report information about the system on which they are used. Information is provided over the Web-Based Enterprise Management (WBEM) industry-standard protocol. A central management server (CMS) using HP Systems Insight Manager (HP SIM) gathers, organizes, and displays the information in reports enabling you to monitor system use and troubleshoot problems.

The management provider package contains a set of provider modules which plug into the HP WBEM Services package. The providers extend the basic functions of the HP WBEM Services package by providing additional information about the hardware and operating system.

The provider package can supply the following categories of information in response to WBEM queries. For more information see the HP WBEM Provider Data Sheets available separately.

- Power supplies: name, ID, description, status, and availability.
- Disk SMART sensors: system, state (online, failed/asserted, or unknown).
- Disk drives: id, capabilities, size, block size.
- Disk partitions, logical systems, and logical disks: id, bootable, and type.
- Physical memory: description, bank label, capacity, and memory type.
- Physical memory statistical information: single bit errors, double bit errors, and predictive failure indicator.
- Network adapters: address, speed, maximum speed, duplex indicator, and count of octets transmitted and received.
- PCI systems: id, vendor, grant time, and latency.
- Physical media: name, hot swap capability, capacity, manufacturer, model, serial number, version, and other information.
- SCSI controllers: id, name, description, and protocol.

HP WBEM Providers are available from the Linux link at <http://www.software.hp.com>. WBEM Providers for other HP equipment and operating systems are also available separately.

WBEM is a replacement for the SNMP network management protocol. WBEM providers perform a similar role to SNMP agents of publishing information about a managed system. HP Integrity servers can also be remotely managed using the HP SNMP Agents, which are available separately from <http://www.software.hp.com>.

Caution:



The current release of HP WBEM Providers cannot coexist with the HP Insight Management Agent. This restriction will be removed in a future release. HP recommends Insight Management Agent be installed on production machines.

managed using SNMP, and the HP WBEM Providers be installed for evaluation of WBEM only.

Go to

<http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=WBEMLINUX> for additional information about WBEM Providers for Linux.

Available MSA Tools

The following is a list of the MSA tools available in HP Systems Insight Manager (HP SIM):

- Deploy SSH Public Key
- Ignite-UX Console
- Ignite-UX Restricted Console
- Create or Modify Recovery Archive
- Create or Modify Tape Recovery Archive
- Install or Recover System
- PostgreSQL DB Backup
- Install Software
- Remove Software
- Software Distributor Job Browser
- Copy Depot Software
- Remove Depot Software
- SD Job Browser
- Subscribe to WBEM Events
- Install WLM Configuration
- Retrieve WLM Configuration
- Syntax Check on the Systems Insight Manager Server Configuration
- Syntax Check Configuration
- Install OpenSSH
- Initial ProLiant Support Pack Install
- Install Software and Firmware

Partner Applications

HP Systems Insight Manager (HP SIM) partner applications extend the breadth of HP system coverage and improve the lifecycle management capabilities for your HP servers as plug-in tools or TDEF files.

Note:



If you are looking for information on a tool that is not listed on this page or referenced in this help system, then it might be a custom tool or a tool provided by a company other than HP. Ask your administrator for assistance.

HP Integrity Essentials Plug-ins

Feature	HP Product	HP-UX	Linux	Windows	OpenVMS
Configuration Management	Availability Manager				X
	HP-UX Bastille [useTools_plugins_HPUBastille.html#HPUBastille]	X			
	HP-UX Webmin-based Admin [useTools_webmin.html#webmin]	X	X	X	X
	Integrated Lights-Out [useTools_plugins_IOIntegServices.html#IOInteg]	X	X	X	X
	Management Processor [useTools_mgmtProc.html#mgmtProc]	X	X		
	Partition Manager [useTools_partitionMgr.html#pm]		X	X	
	HP Serviceguard Manager [useTools_SGCluster.html#SGMgr]				
	System Management Homepage/SAM [useTools_systemInfo_smhp.html#smh]				

Feature	HP Product	HP-UX	Linux	Windows	OpenVMS
Software Deployment	Linux Enabled Kit		X		
	Ignite-UX [useTools_plugins_igniteUX.html#igniteUX]	X			
	Security Patch Check [useTools_securityPatchCheck.html#securityPatch]	X		X	
	Smartsetup CD	X			
	Software Distributor-UX [useTools_plugins_softwareDistributor.html#sdl]	X			X
	Software Package Builder				
	VMS Loader				
Virtualization and Automation Management	Class Scheduler				X
	Global Workload Manager	X	X		
	HP-UX Workload Manager	X			
	OpenView GlancePlus [useTools_plugins_glancePlusPak.html#gpp]	X	X		
	OpenView Performance Agent	X	X	X	X
	Process Resource Manager [useTools_prm.html#prm]	X			

HP ProLiant Essentials Plug-ins

Feature	Description
Central Management	<ul style="list-style-type: none"> ● Integrated Lights-Out Advanced Pack. Control ProLiant servers remotely through a Web browser ● Intelligent Networking Pack. Minimize the risk of outages due to network failures or virus attacks

Feature	Description
Configuration Management	<ul style="list-style-type: none"> ● Performance Management Pack [useTools_pmp.html#pmp] . Identify systems with performance bottlenecks ● Rack and Power Manager. Grow with your datacenter demands for power protection and rack space ● HP BladeSystem Integrated Manager [useTools_plugins_bladeSystem.html#bladeSystem] . Access all tools needed to configure and manage an HP BladeSystem environment ● Insight Management Agents. Review in-depth system hardware configuration and status data, performance metrics, system thresholds, and software version control information
Software Deployment	<ul style="list-style-type: none"> ● Rapid Deployment Pack. Automate unattended deployment of HP BladeSystem and ProLiant hardware ● Vulnerability and Patch Management Pack [useTools_plugins_vpm.html#vpm] . Identify and close security vulnerabilities before they result in unplanned downtime ● Server Migration Pack [useTools_smp.html#smp] . Convert between physical and virtual, virtual and virtual, and virtual and physical systems
Virtualization and Automation Management	<ul style="list-style-type: none"> ● Virtual Machine Management Pack [useTools_vmm.html#vmm] . Manage virtual machines in the same manager that you manage your physical machines ● Workload Management Pack [useTools_workloadMgr.html#wlMgr] . Control and dynamically allocate system resources

HP Storage Essentials Plug-ins

Feature	Description
Central Management	<ul style="list-style-type: none"> ● Oracle Viewer. Oracle database availability and performance views ● Exchange Viewer. Oracle database availability and performance views
Application Storage Management	<ul style="list-style-type: none"> ● Sybase Viewer. Sybase database availability and performance views ● SQL Viewer. SQL database availability and performance views
Configuration Management	<ul style="list-style-type: none"> ● Provisioning Manager. Heterogeneous host-to-array path provisioning wizard ● Storage Essentials Enterprise Edition. Main console for open, heterogeneous LAN management ● Chargeback Manager. Assign tiers and create asset-based chargeback management
Reporting	<ul style="list-style-type: none"> ● Provisioning Manager. Heterogeneous host-to-array path provisioning wizard ● Global Reporter. View roll-up reporting of multiple Storage Essentials instances ● Report Designer. Develop customer reports for your storage infrastructure

HP Infrastructure Resource Management Plug-ins

Feature	HP Product	Managed Systems
Client Management Software	<p>HP Client Manager [see Tools, plug-ins, Client Management Software #ClientMg]</p> <p>Web JetAdmin [see Tools, plug-ins, Web JetAdmin #WebAdmin]</p>	<p>HP Business Desktop, Workstation, Notebook, and Tablet PCs</p> <p>HP management supported printers and non-HP network peripherals</p>

Related Topics

- Managing with Tasks
- Viewing Task Results
- Array Configuration Utility Overview
- HP BladeSystem Overview
- HP Client Manager Overview
- Event Monitoring Service Overview
- GlancePlus Overview
- HP-UX Bastille Overview
- Ignite-UX Overview
- Integrated Lights-Out Overview
- HP Integrity Essentials Overview
- HP OpenView Storage Area Management Overview
- HP OpenView Storage Data Protector Overview
- HP OpenView Performance Agent Overview
- HP OpenView Storage Management Appliance Overview
- HP OpenView Storage Operations Manager Overview
- Partition Manager Overview
- HP ProLiant Essentials Automation Manager Overview
- HP ProLiant Essentials Applications
- Software Distributor Overview
- HP Storage Essentials Overview
- HP StorageWorks EVA Overview
- HP StorageWorks Command View SDM Overview
- HP StorageWorks Command View Tape Library Overview
- HP StorageWorks Command View XP Overview
- HP StorageWorks Command View XP Advanced Edition Overview
- HP StorageWorks Modular Storage Array 1000 Overview
- System Fault Management Overview
- ProLiant Essentials Vulnerability and Patch Management Pack Overview
- HP Virtual Server Environment Overview
- WBEM Providers Overview
- Web JetAdmin Overview
- PMP Tools
- Process Resource Manager Overview
- RPM Package Manager
- Security Patch Check Overview
- HP Serviceguard Manager Overview
- Server Migration Pack
- Virtual Machine Management Pack
- Webmin Overview
- Workload Manager Overview

HP Integrity Essentials Overview

HP Integrity Essentials is an optional plug-in for HP Systems Insight Manager (HP SIM) that enables you to add powerful lifecycle features while continuing to benefit from common security and configuration management.

HP SIM and HP Integrity Essentials help you control IT infrastructure with unified management of your HP Integrity server environment running:

- HP-UX 11i
- Windows
- Linux
- OpenVMS

HP Integrity Essentials for HP-UX 11i

HP Integrity Essentials provides modular, integrated system management software for complete Integrity server management for multiple operating systems, including HP-UX 11i.

Software deployment

- Ignite-UX [useTools_plugins_igniteUX.html#igniteUX] for fast deployment
- Software Distributor-UX [useTools_plugins_softwareDistributor.html#softDist] distributes software for HP-UX
- Software Package Builder allows easy updates to HP-UX
- Security Patch Check and Patch Assessment Tool [useTools_securityPatchCheck.html#securityPatch] improves system security

Configuration management

- HP Integrity Essentials Virtualization Manager provides comprehensive, integrated configuration, and management of all Virtual Server Environment elements
- HP Integrity Essentials Capacity Advisor for ongoing capacity planning simulating placement of application workloads
- System Management Homepage (SMH)/ System Administration Manager for basic HP-UX management
- Partition Manager [useTools_partitionMgr.html#pm] to create and manage hard partitions
- HP-UX Bastille [useTools_plugins_HPUBastille.html#HPUBastille] for security hardening /lock down
- HP-UX Webmin [useTools_webmin.html#webmin]-based Admin allows open source tools to plug in
- Serviceguard Manager [useTools_SGCluster.html#SGM] to manage Serviceguard clusters

Workload management

- Process resource manager for workload management
- Secure Resource Partitions for secure application stacking
- HP-UX Workload Manager [useTools_workloadMgr.html#wlMgr] is an intelligent policy engine for the HP Virtual Server Environment

- Global Workload Manager, the intelligent policy engine for multi-system Virtual Server Environments
- OpenView GlancePlus and Performance Agent for performance monitoring

Remote server management

- Integrated Lights-Out (iLO) [useTools_plugins_iLO_integrityServers.html#iLO] for entry level Integrity servers
- Management Processor [useTools_mgmtProc.html#mgmtProc] for mid-range and high-end Integrity servers

HP Integrity Essentials for Windows

Deployment and configuration

- Integrity Essentials Foundation Pack for Windows a complete toolset to install, configure and manage HP Integrity servers with Windows Server 2003.
- Smart Setup CD for easy server configuration and the latest HP drivers, firmware utilities and management assets.
- HP ProLiant Essentials Performance Management Pack [useTools_pmp.html#pmp] to create and manage hard partitions (nPars)
- System Management Homepage (HP Insight Management Agents) provides a consolidated view of an individual server.
- HP Version Control Agent (VCA) and HP Version Control Repository Manager (VCRM) for easy system software maintenance
- NIC Configuration Utility configures and monitors HP Network Interface Controllers.
- HP ProLiant Essentials Performance Management Pack [useTools_pmp.html#pmp] detects and analyzes performance bottlenecks for HP Integrity servers.

Remote server management

- Integrated Lights-Out (iLO) for entry level Integrity servers
- Management Processor for mid-range and high-end Integrity servers

HP Integrity servers with Linux

Central administration

HP SIM is the foundation for HP's unified server-storage management strategy. It is a multiple operating system, hardware level management product that supports HP Integrity, HP ProLiant and HP 9000 servers. HP SIM is easily extensible, integrating other HP management products and value-add plug-ins such as HP Integrity Essentials.

OpenView HP's enterprise-level management solution System Management Homepage (Insight Management Agents) provides a consolidated view of an individual server.

HP Integrity Essentials provides modular, integrated system management software for complete Integrity server management for multiple operating systems, including Linux.

HP Integrity Essentials for Linux

Deployment and Configuration

Enablement Kit for Linux including SystemImager, delivers all the latest and compatible HP drivers, firmware, utilities, and Insight Management Agents; and manages the installation of the operating system

HP Integrity Essentials Capacity Advisor for ongoing capacity planning simulating placement of application workloads

System Management Homepage provides a consolidated view of an individual server

Partition Manager to create and manage hard partitions (nPars) Serviceguard Manager to manage Serviceguard clusters

Workload Management

Global Workload Manager, the intelligent policy engine for multi-system Virtual Server Environments

OpenView GlancePlus and Performance Agent for performance monitoring

Remote server management

Integrated Lights-Out (iLO) for entry level Integrity servers

Management Processor for mid-range and high-end Integrity servers

HP Integrity servers with OpenVMS

Central administration

HP SIM is the foundation for HP's unified server-storage management strategy. It is a multiple operating system, hardware level management product that supports HP Integrity and HP 9000 servers. HP SIM is easily extensible, integrating other HP management products and value-add plug-ins such as HP Integrity Essentials.

OpenView, HP's enterprise-level management solution including OpenView Operations Agent for seamless management from OpenView Operations.

HP Integrity Essentials provides modular, integrated system management software for complete Integrity server management for multiple operating systems, including OpenVMS.

HP Integrity Essentials for OpenVMS

Configuration Management

Availability Manager real-time performance monitor for OpenVMS Insight Management Agents enable HP SIM Partition Manager to create and manage hard partitions (nPars)

Workload Management

Availability Manager real-time performance monitor for OpenVMS

Insight Management Agent enable HP SIM Partition Manager to create and manage hard partitions (nPars)

Remote server management

Integrated Lights-Out (iLO) for entry level Integrity servers

Management Processor for mid-range and high-end Integrity servers

Related Topics

- Partner Applications
- HP BladeSystem Overview
- Event Monitoring Service Overview
- GlancePlus Overview
- HP-UX Bastille Overview
- Ignite-UX Overview
- Integrated Lights-Out Overview
- Management Processor Tools
- HP OpenView Storage Data Protector Overview
- HP OpenView Performance Agent Overview
- Partition Manager Overview
- Process Resource Manager Overview
- Security Patch Check Overview
- HP Serviceguard Manager Overview
- Software Distributor Overview
- Webmin Overview
- Workload Manager Overview

Event Monitoring Service Overview

Event Monitoring Service (EMS) is a system monitoring application designed to facilitate real-time monitoring and error detection for HP products in the enterprise environment. This framework provides centralized management of hardware systems and system resources and provides immediate notification of hardware failures and system status.

HP EMS reports information that helps you detect loss of redundant resources, thus exposing single points of failure and eliminating the threat to data and application availability. HP EMS capabilities cover the entire system: system components, storage, and network interfaces.

To access the Event Monitoring Services in HP Systems Insight Manager (HP SIM), select **Diagnose->Event Monitoring Service**.

Go to <http://docs.hp.com/en/B7612-90015/ch01s01.html> for more information and access to documentation.

HP-UX Bastille Overview

HP-UX Bastille is a security hardening/lockdown tool which can be used to enhance the security of the HP-UX operating system. It provides customized lockdown on a system by system basis, addressing a large number of the recommendations from a number of popular security scanning tools and checklists.

Features and Benefits

- Configures daemons and system settings to be more secure
- Turns off unneeded services such as pwgrd
- Helps create chroot jails that partially limit the vulnerability of common Internet services such as Web servers and Domain Name System (DNS)
- Educates users through its user interface
- Configures Security Patch Check to run automatically
- Configures an IPFilter-based firewall
- The revert feature returns the security configuration to the state before Bastille was run

HP-UX Bastille must be downloaded and installed from the HP website.

Go to

http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6849AA for more information and access to documentation.

GlancePlus Overview

HP OpenView GlancePlus Pak provides you with a single product for managing a system's availability and performance. It is an integrated product that includes:

- HP OpenView GlancePlus
- HP OpenView Performance Agent

As an integrated product, the GlancePlus Pak includes the real-time diagnostic capabilities of GlancePlus and the historical data collection capabilities of the Performance Agent. The performance agent is used with other availability and performance management products, providing an integrated real-time and historical performance management solution.

With GlancePlus Pak, you can handle a wide range of system performance and availability problems to get the best from your system and the applications running on it.

To access GlancePlus Pak, select **Tools->performance monitors**.

Go to <http://www.managementsoftware.hp.com/products/gppak2k/index.html> for more information and access to documentation.

Ignite-UX Overview

Ignite-UX addresses the need for HP-UX system administrators to perform system installations and deployment, often on a large scale. It provides the means for creating and reusing standard system configurations. It provides the ability to archive a standard system configuration, and to use that archive to replicate systems, with the added benefit of speeding up the process. It also permits post-installation customizations, and is capable of both interactive and unattended operating modes.

Note:



This is available for HP-UX systems only.

After Ignite-UX has been installed, you can access its features within HP Systems Insight Manager (HP SIM) by selecting **Deploy->Ignite-UX**.

Go to <http://docs.hp.com/en/IUX/> for more information and access to documentation for Ignite-UX.

Integrated Lights-Out Overview

Basic system management functions, diagnostics and essential Lights-Out functionality are included as core components of Integrated Lights-Out (iLO) supported servers. The standard features of iLO are referred to as iLO Standard. Advanced remote administration functionality, referred to as iLO Advanced, can be licensed with the optional Integrated Lights-Out Advanced Pack for HP Integrity Servers.

iLO functionality on HP Integrity servers is very similar to that offered on HP Pro-Liant servers to ensure a common user experience between HP's ProLiant and Integrity platforms.

The key iLO Standard features on Integrity servers include:

- **Web Graphical User Interface (GUI).** Access the iLO from anywhere using any standard browser
- **Virtual Power.** Full remote control of the server power button
- **Remote text console.** Operating system-independent, text-based console to display and control remote host server activities such as shutdown and start-up
- **Virtual Serial Port.** Access serial port applications such as Windows Server 2003 Emergency Management Services and Text Telephone (TTY) sessions over your LAN
- **Command line and scripting interfaces.** Flexible operation, configuration, and maintenance
- **Secure Sockets Layer (SSL) encryption.** All data transmitted between iLO processors and client browsers
- **iLO and server diagnostics.** Detailed status logs
- **Domain Name System (DNS)/Dynamic Host Configuration Protocol (DHCP).**

- **Remove Firmware Update.**
- **Intelligent Platform Management Interface (IPMI) over LAN.**

The key iLO Advanced Pack features include:

- Directory Services Integration for iLO User Management using Lightweight Directory Access Protocol (LDAP)-based Directory Services
- Secure Shell (SSH encryption) support for secure access to iLO
- iLO Group Actions for managing multiple systems using HP Systems Insight Manager (HP SIM)

Go to <http://h71028.www7.hp.com/enterprise/cache/98327-0-0-0-121.html/> for more information and access to documentation for iLO for HP Integrity servers.

Partition Manager Overview

Partition Manager provides system administrators with a convenient graphical user interface to configure and manage nPartitions on HP server systems. Using Partition Manager, you can perform complex configuration tasks without having to remember commands and parameters. You select nPartitions, cells, I/O chassis, or other components from the graphical display, then select an action from a menu.

With HP Systems Insight Manager (HP SIM), you can:

- Modify nPartitions
- View and Modify nPartitions
- View and Modify Remove Complex

To access the Partition Manager features within HP SIM, select **Tools->Partition Manager**.

Go to <http://docs.hp.com/en/PARMGR2/index.html> for more information and access to documentation.

Security Patch Check Overview

Security Patch Check is a tool that analyzes the currency of a system with respect to security bulletins. It recommends actions for security vulnerabilities that have not been fixed by previously performed patches, updates, removals, or, where logged by the user, manual actions. The actions might include updates, software removals, or manual actions. Use of the Security Patch Check software tool can help efficiently improve system security, but does not guarantee system security.

Features and benefits of Security Patch Check include:

- Generates a report of recommended security actions which are applicable and not installed or applied

Helps automate the process of checking for security patches, updates or manual actions missing from a system

Warns about patches with warnings that are present on the system being analyzed.

Integrates with HP Systems Insight Manager (HP SIM) by enabling you to get the patch catalog and to run Security Patch Check.

To access the Security Patch Check features within HP SIM, select **Configure>Security**.

HP Serviceguard Manager Overview

HP Serviceguard Manager is a graphical user interface that provides configuration, monitoring, and administration of Serviceguard, Serviceguard Extension for RAC, Metrocluster, and Continentalclusters. Using Serviceguard Manager, you get a birds-eye view of the status of all the clusters on your network through color-coded icons. From this high-level perspective, you can drill down and proactively manage specific clusters, nodes, and packages.

Serviceguard clusters are identified and associated through SNMP and provide a mechanism to view cluster information by running HP Serviceguard Manager if it is registered with HP Systems Insight Manager (HP SIM).

Note:



If you have systems that have both SNMP and WBEM Serviceguard cluster awareness agents installed and you previously ran HP SIM 4.x, you must re-run discovery for Serviceguard cluster information to be obtained through WBEM.

There are several ways to access HP Serviceguard Manager:

- From the system table view page, select a system that is an HP Serviceguard Cluster. HP SIM searches the database for the first system that belongs to the cluster and Serviceguard Manager is launched with that system.
- From the system table view page, click a container system that has a cluster member. The cluster member is passed to Serviceguard Manager. You can also select the row that includes the container system and then launch Serviceguard Manager from the menu by selecting **Tools>Integrated Consoles>HP Serviceguard Manager**.
- From the system table view page, click a cluster node. The cluster node is passed to Serviceguard Manager. You can also select the row that includes the container system and then launch Serviceguard Manager from the menu by selecting **Tools>Integrated Consoles>HP Serviceguard Manager**.
- Access the **HP Serviceguard Manager** page by selecting **Tools>Integrated Consoles>HP Serviceguard Manager**. The **HP Serviceguard Manager** page appears.

Note:



If you have not used HP Serviceguard Manager prior to HP SIM (HP SIM) 5.0, you can download the latest version from: <http://www.hp.com/go/softwaredepot> and click **HP Serviceguard Manager**. When you install HP Serviceguard Manager, it recognizes HP SIM and automatically registers it for you. If you used HP Service

Manager 4.02 with previous versions of HP SIM, when you upgrade to HP SIM to 5.0, the tool HP Serviceguard Manager 4.02 is still available.

Go to <http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B8325BA> for more information and to download the software.

Related Topics

- Navigating the System Table View Page
- Navigating the Cluster Table View Page

Software Distributor Overview

Software Distributor (SD) is the HP-UX administration tool set used to deliver and maintain HP-UX operating systems and layered software applications. SD is delivered as part of HP-UX; you do not need to download it separately.

SD works with you. System administrators use SD to manage software on HP PA-RISC and Itanium®-based systems. Software packagers use SD to organize, standardize and distribute software to customers. HP-UX partners use SD as the primary tool for building and testing complete solutions for the enterprise and technical desktop.

Note:



This is available for HP-UX systems only.

To access SD through HP Systems Insight Manager (HP SIM), select **Deploy->Software Distributor**.

To view SD logs, select **Tasks & Logs->View Software Distributor Agent Log** and **Tasks & Logs->View Software Distributor Daemon Log**.

Go to <http://www.docs.hp.com/en/SD/> for more information and access to documentation.

Webmin Overview

Webmin is a Web-based interface for system administration for UNIX and is also used with Linux. Using HP Systems Insight Manager (HP SIM), you can set up user accounts, Apache, DNS, file sharing and so on. Webmin consists of a miniserver, and many Common Gateway Interface (CGI) programs, which directly update system files like `/etc/inetd.conf` and `/etc/passwd`. The Web server and all CGI programs are written in Perl 5 and use no external modules, which means that you only need a Perl binary to run Webmin.

Because Webmin supports the concept of modules (for example, PhotoShop plugins), you can develop and distribute your own Webmin modules for any purpose, and distribute them under any license (such as General Public License (GPL), commercial, or shareware).

To access Webmin in HP SIM, select **Tools->Integrated Consoles->Webmin**. The **Webmin** page appears. Select a target system and click **Run Now**.

Workload Manager Overview

HP-UX Workload Manager (HP-UX WLM) is a resource management tool that provides automatic CPU resource allocation and application performance management based on prioritized service-level objectives (SLOs). In addition, real memory and disk bandwidth allocations can be set to fixed levels in the configuration.

The following features are available within HP Systems Insight Manager (HP SIM):

- Workload Manager Console
- Activate WLM Configuration
- Enable WLM
- Install WLM Configuration
- Restart WLM
- Stop WLM
- Syntax Check Configuration
- Syntax Check on HP SIM Configuration
- Truncate Statistics Log Files
- View Workload Manager Log Files
- View Workload Manager Statistics Log Files
- Ability to Launch Workload Manager from the GUI

To access the Workload Manager features within HP SIM, select **Optimize->Workload Manager, Tasks & Logs->Workload Manager Log Files**, and **Tasks & Logs->Workload Manager Statistics Log Files**.

Go to <http://www.hp.com/products1/unix/operating/wlm/overview.html> for more information.

HP OpenView Storage Data Protector Overview

HP OpenView Storage Data Protector is software that manages backup and recovery from both disks and tapes, delivering maximum data protection while providing continuous business operations. The software is designed to simplify and to centralize backup and recovery operations by integrating a variety of techniques to eliminate backup windows. These range from on-line backup, open file backup, and instant recovery or zero-downtime backups. Its proven industry-leading instant recovery features and several other integrated disaster recovery alternatives meet the demands of the most complex enterprises so that they can recover critical data within minutes.

Data Protector simplifies the use of complex backup and recovery procedures with the fastest installation, automated routine tasks, and easy-to-use features. The ideal solution to reduce complexity while remaining reliable and scalable to grow from single server environments to the largest

distributed enterprise infrastructures, providing broad compatibility of operating systems, applications, drives, libraries, and disk arrays.

It also provides tracking and management of offline storage media. Maximizing media operations productivity and increasing data availability by automating the tracking and management of removable storage media. With media operations, customers can manage the complete life cycle of removable storage media; shortening recovery time, reducing financial and business risks from lost data, and minimizing opportunities for human error.

HP OpenView Storage Data Protector is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page** only after the application has been installed. Refer to “Tools & Links Tab” for information on accessing the **System Page**.

Go to <http://h18006.www1.hp.com/products/storage/software/dataprotector/index.html> for more information and access to documentation.

HP OpenView Performance Agent Overview

The HP OpenView Performance agent logs and collects data, then sends alarms about that data when necessary. The agent is installed on each system you plan to monitor.

With its powerful end-to-end application response measurement capabilities, the Performance agent is the core enabling technology in any service management strategy.

HP OpenView Performance Agent must be downloaded and installed from the HP website.

Go to <http://www.managementsoftware.hp.com/products/ovperf/index.html> for more information and access to documentation.

HP OpenView Storage Area Management Overview

HP OpenView Storage Area Manager software simplifies and automates the management of your storage resources and infrastructure. Storage Area Manager has a modular building block architecture consisting of five functional modules: Storage Node Manager, Storage Builder, Storage Optimizer, Storage Accountant, and Storage Allocator. From its central console, it enables you to selectively monitor, manage, optimize, and plan storage service availability, performance, usage, cost, and growth. Storage Area Manager also enables management and planning for capacity related to Oracle and Microsoft Exchange applications.

This helps increase administrator efficiency and reduces the cost of managed storage. Storage Area Manager helps you define, monitor, and measure storage service levels enabling the creation of storage utility. It enables management and control of storage and applications to support the Adaptive Enterprise. Its integration with third-party reporting tools and Enterprise management tools helps deliver an integrated IT service. Storage Area Manager support for Storage Management Initiative-Specifications (SMI-S) based systems protects investment while reducing complexity and increasing freedom of choice in a heterogeneous environment.

HP OpenView Storage Area Manager is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. Refer to “Tools & Links Tab” for information on accessing the **System Page**.

Go to <http://h18006.www1.hp.com/products/storage/software/sam/index.html> for more information and access to documentation.

HP OpenView Storage Management Appliance Overview

The HP OpenView Storage Management Appliance is a centralized, appliance-based monitoring and management solution for the SAN. Connected directly to the fabric, it performs management functions outside of the data path and without involving host computers, allowing data transfers to proceed independently between computers and storage systems.

The Storage Management Appliance optimizes SAN availability and performance while streamlining manageability by enabling policy-based automation of repetitive storage management tasks. It provides an intuitive, web-based interface and storage management aggregation point enabling the user to organize, configure, visualize, monitor, and provision storage from anywhere, anytime. The Storage Management Appliance includes HSG Element Manager and provides support for HP OpenView Storage Operations Manager. This combined solution delivers easy-to-use tools for centralized management of Enterprise Virtual Array and EMA/MA Arrays on the SAN, as well as the foundation for comprehensive enterprise storage resource management across multi-vendor platforms in the network storage infrastructure.

The Storage Management Appliance supports a variety of additional value-added storage management applications from HP, as well as popular virus protection, backup, system management, and UPS software products.

- Unobtrusive, centralized appliance for storage management

The HP OpenView Storage Management Appliance provides an unobtrusive, centralized point for managing and monitoring the SAN and other networked storage systems. Designed to connect directly to the SAN fabric, the Storage Management Appliance performs management functions without involving host computers.

- Optimizes SAN availability and performance

Strategically located out of the SAN data path, the Storage Management Appliance enables data transfers to proceed independently between computers and storage systems whether it is operating or not. The Storage Management Appliance optimizes SAN availability and performance while streamlining SAN manageability.

- Web-based interface for storage management

Included with the Storage Management Appliance, HP OpenView Storage Management Appliance software provides a Web-based aggregation and entry point for centralized storage management. This intuitive interface enables the user to organize, visualize, configure, and monitor storage from a single navigation point on the SAN. Storage Management Appliance software provides a launch site for a variety of value-added HP storage management applications, and provides navigation links to directly manage storage components on the SAN.

- HSG Element Manager

This easy to use, graphical storage configuration and monitoring tool centralizes storage management across network and multivendor platforms. Included with the HP OpenView Storage Management Appliance, HSG Element Manager reduces the job of storage management to simple point-and-click, across the switched Fibre Channel SAN. It provides for easy configuration of HP StorageWorks HSG80/60 storage systems as well as field replaceable unit (FRU) level fault detection and notification, through an SNMP agent with MIB event logging. This new

version introduces a provider for the Storage Networking Industry Association Storage Management Initiative Specification (SMI-S), enabling greater multi-vendor manageability in the enterprise network storage infrastructure.

HP OpenView Storage Management Appliance is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. Refer to “Tools & Links Tab” for information on accessing the **System Page**.

Go to <http://h18006.www1.hp.com/products/sanworks/managementappliance/index.html> for more information and access to documentation.

HP OpenView Storage Operations Manager Overview

HP OpenView Storage Operations Manager is a comprehensive and efficient EVA and SAN management solution, combining into one offering the power of Command View EVA and Storage Node Manager from the HP OpenView Storage Area Manager suite. Storage Operations Manager will identify, configure, monitor, and manage HP StorageWorks EVAs in a single SAN and across distributed heterogeneous implementations. Its system discovery technology also automatically identifies and visually monitors other heterogeneous storage systems from a central console, including network storage (SAN and NAS), direct-attached storage, and their infrastructure. With the Storage Operations Manager solution, the foundation and core services for HP OpenView Storage Area Manager (SAM) are installed, enabling administrators to easily extend the solution to include performance management, usage, cost, and growth management for EVAs, disk, tape, direct-attached, and network storage infrastructures as an option. HP OpenView SAM software optimizes resource utilization, increases administrator efficiency and reduces cost of managed storage ownership.

HP OpenView Storage Operations Manager is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. Refer to “Tools & Links Tab” for information on accessing the **System Page**.

Go to <http://h18006.www1.hp.com/products/storage/software/som/index.html> for more information and access to documentation.

Process Resource Manager Overview

HP's Process Resource Manager (PRM) enables the system administrator to focus the appropriate amount of system resources exactly where the business needs them. This powerful resource management tool runs as an addition to the HP UNIX operating system (HP-UX). When PRM is enabled, groups of users or applications are guaranteed a specified portion of the total system central processing unit (CPU) processing cycles, of the available real memory resources, and of the disk bandwidth to logical volume-managed (LVM) systems.

PRM is a resource management tool used to control the amount of resources that processes use during peak system load (at 100% CPU, 100% memory, or 100% disk bandwidth utilization). PRM can guarantee a minimum allocation of system resources available to a group of processes through the use of PRM groups.

A PRM group is a collection of users and applications that are joined together and assigned certain amounts of CPU, memory, and disk bandwidth. The two types of PRM groups are FSS PRM groups and PSET PRM groups. An FSS PRM group is the traditional PRM group, whose CPU entitlement is specified in shares. This group uses the Fair Share Scheduler (FSS) in the HP-UX kernel within the system's default processor set (PSET). A PSET PRM group is a PRM group whose CPU entitlement

is specified by assigning it a subset of the system's processors (PSET). Processes in a PSET have equal access to CPU cycles on their assigned CPUs through the HP-UX standard scheduler.

Reasons to Use PRM

- Improve the response time for critical users and applications.
- Set and manage user expectations for performance.
- Allocate shared servers based on budgeting.
- Ensure that an application package in a Serviceguard cluster has sufficient resources on an active standby system in the event of a failover.
- Ensure that critical users or applications have sufficient CPU, memory, and disk bandwidth resources.

Users who at times run critical applications, might at other times engage in relatively trivial tasks. These trivial tasks can be competing in the users' PRM group with critical applications for available CPU and real memory. For this reason, it is often useful to separate applications into different PRM groups or create alternate groups for a user. You can assign a critical application its own PRM group to ensure that the application gets the needed share of resources.

- Restrict the CPU, real memory, and disk bandwidth resources available to relatively low-priority users and applications during times of heavy demand.

For example, mail readers can consume significant disk bandwidth when users first come into work or return from lunch. Therefore, you might want to assign an application like mail to a PRM group with small resource allocations and restrict the amount of resources mail can use during such times of heavy demand on the system.

- Monitor resource consumption by users or applications.

Assigning a group of users or applications to separate PRM groups can be a good way to keep track of the resources they are using.

Accessing Process Resource Manager From HP SIM

Select **Optimize>Process Resource Manager**. There are three options available:

- Process Resource Manager Console
- Display Resource Usage
- List Resource Availability
- Launch PRM fro the GUI

Go to: <http://www.hp.com/go/prm> for more information on PRM.

HP ProLiant Essentials Applications

HP ProLiant Essentials includes software to assist in managing your ProLiant servers. ProLiant Essentials Services can help you:

- Contain server-related acquisition and operating costs
- Reduce the risks associated with change
- Improve overall IT manageability
- Decrease application downtime by speeding problem detection and resolution
- Increase service efficiency and productivity

The applications listed here are considered partner applications with HP Systems Insight Manager (HP SIM) and are all available automatically with an installation of HP SIM or by download from the HP website.

Monitor and Alert

- HP BladeSystem Integrated Manager
- HP Intelligent Networking Pack
- HP Insight Management Agent

Analyze and Control

- HP Power Regulator
- HP ProLiant Essentials Performance Management Pack
- Insight Diagnostics
- Workload Management Pack

Provision and Patch

- HP Array Configuration Utility
- HP BladeSystem Setup through iLO
- ProLiant Support Pack
- Rapid Deployment Pack
- SmartStart Scripting Toolkit
- HP ProLiant Essentials Vulnerability and Patch Management Pack

Recovery and Scale

- HP ProLiant Essentials Server Migration Pack
- HP ProLiant Essentials Virtual Machine Management Pack
- VMware+ProLiant Essentials Bundle

Remote Management

- Integrated Lights-Out Standard Edition
- Integrated Lights-Out Advanced Edition
- Lights-Out 100 Remote Management
- Remove Insight Lights-Out Edition II

Enterprise Management

- HP OpenView Storage Data Protector
- HP OpenView Storage Management Appliance
- HP OpenView Storage Operations Manager

Other HP Management

- HP Client Manager
- HP OpenView Storage Area Management
- Web Jetadmin

For more information on HP ProLiant Essentials and links to the above partner applications, go to <http://h18013.www1.hp.com/products/servers/management/index.html>.

Related Topics

- HP ProLiant Essentials Automation Manager Overview
- PMP Tools
- ProLiant Essentials Vulnerability and Patch Management Pack Overview
- Array Configuration Utility Overview
- Virtual Machine Management Pack
- Server Migration Pack
- Management Processor Tools
- HP OpenView Storage Area Management Overview
- HP OpenView Storage Management Appliance Overview
- HP OpenView Storage Operations Manager Overview
- Workload Manager Overview
- HP BladeSystem Overview
- RPM Package Manager
- Web JetAdmin Overview
- HP Client Manager Overview

Array Configuration Utility Overview

The HP Array Configuration Utility (ACU) software for Smart Array controllers and the StorageWorks Enclosure 4x00 family of products makes it easy to configure and expand your disk drive arrays. This Web based tool is very intuitive. By using its Configuration Wizards, your array controller is setup and ready to use in minutes. ACU is also versatile: use it to locally or remotely configure your

array controller, add additional disk drives to an existing configuration, or completely reconfigure your disk drive array. Additionally, innovative features such as Online Capacity Expansion, Logical Drive Capacity Extension, and RAID Level Migration enable you to change your array configuration and settings as your storage needs change.

HP Array Configuration Utility is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. Refer to “Tools & Links Tab” for information on accessing the **System Page**.

Go to

<http://h18000.www1.hp.com/products/servers/proliantstorage/software-management/acumatrix/index.html> for more information.

HP ProLiant Essentials Automation Manager Overview

The HP ProLiant Essentials Automation Manager automates and enables the policy-based, end to end provisioning of the HP BladeSystem Integrated Manager in HP Systems Insight Manager through a wizard-driven provisioning and deployment process. It also enables automated server blade recovery through user-established policies.

The HP ProLiant Essentials Automation Manager integrates with the HP BladeSystem Integrated Manager in HP Systems Insight Manager in HP Systems Insight Manager (HP SIM), which provides a consolidated view to manage all your HP blade components, including HP blades, switches, enclosures, and racks. The HP ProLiant Essentials Automation Manager also integrates with the HP ProLiant Essentials Rapid Deployment Pack - Windows Edition, which combines HP and Altiris software to automate the deployment and provisioning of server software.

The HP ProLiant Essentials Automation Manager and the HP BladeSystem Integrated Manager in HP Systems Insight Manager are plug-in products to HP SIM 4.2 and 5.0 that enable ease of use, installation, and maintenance. These products install and run on the HP SIM central management server.

The HP ProLiant Essentials Automation Manager provides:

- End to end provisioning with automatic deployment based on group membership
- Automated provisioning based on collections
- Server recovery based on fault-notification

If installed, HP ProLiant Essentials Automation Manager is available in HP SIM by selecting:

- **Tools->Automation and Options->Automation Settings->Manage Automation.**

or

- **Tools->Automation and Options->Automation Settings->Pending Automation Actions.**

Go to HP ProLiant Essentials Automation Manager at

<http://www.hp.com/servers/proliantessentials/automation> for more information and refer to the *HP ProLiant Essentials Automation Manager Management Guide* for more information.

Related Topics

- Partner Applications

- HP BladeSystem Overview

HP BladeSystem Overview

HP is delivering HP BladeSystem Integrated Manager as a component in HP Systems Insight Manager (HP SIM) to provide streamlined management access for the HP BladeSystem Integrated Manager in HP Systems Insight Manager. The HP BladeSystem Integrated Manager in HP Systems Insight Manager is comprised of blade computer nodes, integrated connectivity to data and storage networks, and shared power subsystems. The HP BladeSystem Integrated Manager in HP Systems Insight Manager integrated management environment enables users to quickly navigate their HP blade environments including blades servers and desktops, enclosure infrastructures, racks, and integrated switches, through hierarchical tree views. Users are able to conveniently configure, deploy, and manage individual or groups of blade systems. Additionally, users are able to quickly set up logical groups of blade systems for convenient management and control. Finally, the HP BladeSystem Integrated Manager in HP Systems Insight Manager integrated management environment works seamlessly within the expanding HP SIM environment, including ProLiant Essential Value Packs and third party plug-ins to HP SIM. Version 2.0 of HP BladeSystem Integrated Manager in HP Systems Insight Manager is installed automatically with HP SIM 5.0. HP BladeSystem Integrated Manager in HP Systems Insight Manager builds on the current leading capabilities in HP SIM for managing blades, including automatically-generated, interactive blade system rack views.

HP BladeSystem Integrated Manager in HP Systems Insight Manager is available by selecting **Tools->Integrated Consoles->HP BladeSystem**.

Go to <http://h18004.www1.hp.com/products/servers/management/bsme/index.html> for more information and refer to the *HP BladeSystem Integrated Manager in HP Systems Insight Manager Management Guide* for more information.

HP Client Manager Overview

HP Client Manager is the foundation for all of the HP Client Management Solutions providing:

- The infrastructure, data repository, and Web-based console for the other HP Client Management Solutions from Altiris
- Task-based user interface, improved QuickStart screen, streamlined setup and installation for faster software productivity
- Support for HP business desktops, notebooks, and workstations
- Integration with HP Systems Insight Manager (HP SIM) for client hardware management from HP SIM console
- Ability to configure Wake on LAN (WOL) to remotely manage HP PCs even when they are powered off
- Scalable Web-based hardware and BIOS management for HP and Compaq clients
- Complete hardware inventory down to the component level
- Hardware change notification
- Client health monitoring and proactive diagnostics
- Update management (intelligent softppaq distribution/BIOS flashing)

HP Client Manager is available through HP SIM, after being downloaded and installed, from the **Tools->Integrated Consoles->HP Client Manager Console**.

Go to http://h18000.www1.hp.com/im/client_mgr.html for information and access to documentation.

ProLiant Essentials Vulnerability and Patch Management Pack Overview

Gain the upper hand against hackers, worms, and Trojans that exploit software security vulnerabilities, using the HP ProLiant Essentials Vulnerability and Patch Management Pack, the all-in-one vulnerability assessment and patch management tool integrated into HP Systems Insight Manager (HP SIM), simplifying and consolidating the proactive identification and resolution of issues that can impact server availability into one central console.

Vulnerability and Patch Management Pack delivers comprehensive vulnerability assessment and advanced patch management features to accelerate the remediation of vulnerabilities and reduces the risk of exploits.

Vulnerability and Patch Management Pack is available from the **VPM** column on the system table view page. Refer to “Navigating the System Table View Page” for more information.

Go to <http://www.hp.com/servers/proliantessentials/vpm> for more information and access to documentation.

HP Virtual Server Environment Overview

The HP Virtual Server Environment encompasses a number of fully integrated, complementary components that enhance the functionality and flexibility of your server environment.

The following are key HP Virtual Server Environment applications:

- **HP Integrity Essentials Virtualization Manager.** Virtualization Manager is easy-to-use virtualization management software that reduces complexity by providing unified visualization and management of physical and virtual servers. Virtualization Manager provides a central point of control that allows you to manage all the resources in your Virtual Server Environment (VSE). It is a powerful way to connect IT resources to real business needs.
- **HP Integrity Essentials Global Workload Manager (gWLM).** Global Workload Manager (gWLM) is a multi-system, multi-operating system workload manager that serves as an intelligent policy engine in the HP Virtual Server Environment. It simplifies the deployment of automated workload management policies across multiple HP-UX 11i or Linux servers and provides centralized monitoring and reporting providing improved server utilization and maintaining service levels. HP Global Workload Manager is available for HP-UX 11i and Linux.
- **HP Integrity Essentials Capacity Advisor.** HP Integrity Essentials Capacity Advisor is the industry’s first lightweight, integrated tool for ongoing capacity planning, simulating placement of application workloads to help IT administrators improve server utilization. Capacity Advisor provides planning capability for the intelligent control of the HP Virtual Server Environment.
- **HP Systems Insight Manager (HP SIM).** HP Systems Insight Manager (HP SIM) combines the best of Insight Manager 7, HP Tootools, and HP Servicecontrol Manager to deliver

hardware fault, asset, and configuration management for all of your HP Systems. HP SIM can be easily extended to deliver rapid deployment and performance management for workload and partition management for Integrity and HP 9000 systems.

Go to HP Virtual Server Environment at <http://www.hp.com/go/vse> for more information and access to documentation.

Web JetAdmin Overview

HP Web Jetadmin is a simple peripheral management software for remotely installing, configuring, and managing a wide variety of HP and non-HP network peripherals using only a standard Web browser. It can be used to proactively solve problems before they impact user productivity.

HP Web Jetadmin is available through HP Systems Insight Manager (HP SIM), after being downloaded and registered, from the **Tools->Integrated Consoles->WebJet Admin**.

Go to

http://h10010.www1.hp.com/wwpc/pscmisc/vac/us/en/sm/network_software/wjareport_overview.html for more information and access to documentation.

HP Storage Essentials Overview

HP Storage Essentials is a suite of value-added plug-ins that offer advanced heterogeneous storage management functionality including SAN management, storage resource management, provisioning, and application infrastructure monitoring. HP Storage Essentials includes a core product and the following modules:

- **Enterprise Edition.** Main console for open, heterogeneous SAN management
Note: Enterprise Edition is required to have access to the remaining modules.
- **Provisioning Manager.** Heterogeneous host-to-array path provisioning wizard
- **Chargeback Manager.** Asset-based chargeback management. Tier assignment.
- **Oracle Viewer.** Oracle database availability and performance views.
- **Exchange Viewer.** Exchange database availability and performance views.
- **Sybase Viewer.** Sybase database availability and performance views
- **File System Viewer.** File system scanning - reclaim wasted space
- **Global Reporter.** Roll-up reporting of multiple HP Storage Essentials Server instances
- **Report Designer.** Develop customer reports for storage infrastructure

Storage Essentials uses the latest industry standards such as J2EE, SMI-S, WBEM and WMI. This ensures that your storage management infrastructure is extendable and will support both HP and third-party technology, which allows you to use the technology appropriate to your needs and avoid vendor lock-in.

HP Storage Essentials is available through HP Systems Insight Manager (HP SIM) from the **Tools, Deploy, Diagnose, Optimize, Reports, Tasks & Logs**, and **Options** menus. Refer to your HP Storage Essentials documentation for details about these menu items.

Refer to “Changes to HP Systems Insight Manager Storage Functionality when HP Storage Essentials is Installed” for information about the changes that occur in HP SIM when HP Storage Essentials is installed.

Related Topics

- HP StorageWorks EVA Overview
- HP StorageWorks Command View SDM Overview
- HP StorageWorks Command View Tape Library Overview
- HP StorageWorks Command View XP Overview
- HP StorageWorks Command View XP Advanced Edition Overview
- HP StorageWorks Modular Storage Array 1000 Overview

HP StorageWorks Command View XP Overview

HP StorageWorks Command View XP provides centralized, Web-based management for XP disk arrays. It enables collaboration among global team members, eliminating the need for travel to remote locations and increasing the efficiency of your administrator.

Graphical mapping and Fibre Channel diagnostic capabilities provide early warning to conditions that might be hampering the performance of HP storage, ensuring that your data is always available. And Command View contains SNMP scripts, making it easy to integrate into leading network management frameworks.

HP StorageWorks Command View XP is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. Refer to “Tools & Links Tab” for information on accessing the **System Page**.

Go to

http://www.hp.com/products1/storage/products/disk_arrays/xpstorgesw/commandview/index.html for more information and access to documentation.

HP StorageWorks Command View XP Advanced Edition Overview

HP StorageWorks Command View XP Advanced Edition for XP disk arrays combines the best features of Command View XP together with additional Wizard-based ease of use modules. It provides for seamless integration into higher level management utilities such as Storage Essentials. It can centrally manage, configure, provision and monitor XP disk arrays.

HP StorageWorks Command View XP Advanced Edition for XP disk arrays is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. Refer to “Tools & Links Tab” for information on accessing the **System Page**.

HP StorageWorks Command View SDM Overview

HP StorageWorks Command View SDM acts as a centralized management platform through a common user interface from which the value-added software solutions can be launched. Command View scalability ranges from management of a single array to multiple arrays all from a single management console. Command View SDM provides customers with a choice of user interfaces: GUI, CLI or web-browser. Included in Command View SDM is event/trap forwarding capabilities to network management frameworks enabling network administrators to be aware of any changes

in their storage environment. Customers can also link with HP Systems Insight Manager (HP SIM) for initial consolidation of their storage and server environments. Command View SDM supports the emerging SMI-S storage standard reducing manual integration for basic management capabilities.

Command View has been integrated with higher level management frameworks such as OpenView Storage Area Manager for SAN management, OpenView Network Node Manager, CA Unicenter TNG, BMC Patrol, and Tivoli NetView. These integrations empower the network administrator by providing the ability to manage HP storage devices from the customer's network management console.

HP StorageWorks Command View SDM is available through HP SIM from the **Tools & Links** tab on the **System Page**. Refer to "Tools & Links Tab" for information on accessing the **System Page**.

Go to

http://www.hp.com/products1/storage/products/disk_arrays/modular/commandview/index.html for more information and access to documentation.

HP StorageWorks Command View Tape Library Overview

HP StorageWorks Command View Tape Library Software is the next step in the HP Extended Tape Library Architecture (ETLA), a key component of the HP Adaptive Infrastructure strategy. This software delivers tape libraries that are both self-aware and self-managed, automatically maintained, continuously available, network-aware, resilient, secure, and adaptable. The HP tape libraries provide the reliability, interoperability, and advanced functionality required for enterprise SAN environments.

HP StorageWorks Command View Tape Library Software is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. Refer to "Tools & Links Tab" for information on accessing the **System Page**.

Go to <http://h18006.www1.hp.com/products/storageworks/tlarchitecture/index.html> for more information.

HP StorageWorks EVA Overview

HP StorageWorks Command View EVA v4.0 is a comprehensive software suite designed to simplify, enhance, and maximize the high performance HP StorageWorks Enterprise Virtual Array (EVA) family of storage array products.

Command View EVA provides simplicity without compromise as it complements the HP StorageWorks Enterprise Virtual Array user. It offers storage administrators a single storage management solution for all your Enterprise Virtual Array management needs. It automates and aggregates storage management so you have fewer steps to think about and fewer things to manage. Growing capacity is simple, as you can easily and dynamically expand LUNs and add physical drives online to quickly meet changing business needs without application downtime. Provides easy and fast configuration of (LUNs) and RAID groups. For mission critical applications you can take advantage of proactive remote services using the HP Instant Support Enterprise Edition and HP Solutions support to ensure continuous EVA uptime.

HP StorageWorks Command View EVA is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. Refer to "Tools & Links Tab" for information on accessing the **System Page**.

Go to <http://h18006.www1.hp.com/products/storage/software/cmdvieweva/index.html> for more information and access to documentation.

HP StorageWorks Modular Storage Array 1000 Overview

The HP StorageWorks Modular Smart Array 1000 (MSA1000) is a 2 Gb Fibre Channel storage system for the entry-level to midrange storage area network (SAN). It is designed to reduce the complexity and risk of SAN deployments. The powerful but easy to use management software makes it ideal for departmental and remote location SANs. With the addition of two more drive enclosures and the new 300GB drives, it can control up to 42 drives allowing capacity of twelve terabytes. All configuration, management and partitioning and licensing software come standard with no extra charges.

HP's exclusive optional embedded 8-port SAN switches or 3-port hubs give cost effective and space saving methods of creating a SAN environment. The MSA1000 supports Windows (32 & 64-bit), NetWare, and Linux (32 & 64-bit) operating systems. It also supports Tru64 UNIX, OpenVMS, or HP-UX operating systems.

HP StorageWorks Modular Smart Array 1000 is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. Refer to "Tools & Links Tab" for information on accessing the **System Page**.

Go to <http://h18006.www1.hp.com/products/storageworks/msa1000/index.html> for more information and access to documentation.

Reporting

HP ProLiant Essentials Performance Management Pack Reporting

PMP reports are available through HP Systems Insight Manager (HP SIM) on Windows systems. Refer to “PMP Reporting Options” for more information.

To view the System Information Reporting options:

Select **Reports->Performance Management Pack Reports->Static Analysis Report**.

System Information Reporting

The HP SIM System Information Reporting feature enables you to generate reports. In addition to generating reports, you can create customer-defined report configurations and edit, copy, and delete report configurations. All users with login access to HP SIM can generate reports.

Note:



To add a new report, refer to “Adding a Report”.

The System Information Reporting feature provides you with the following options:

- **Managing Reports.** Select **Reports->Manage Reports**. The **Manage Reports** page appears.
- **Running Reports.** Select **Reports->Manage Reports**. The **Manage Reports** page appears. Select the report that you want to run. Select the report format **HTML**, **XML** or **CSV**. Click **Run Report**.
- **Creating New Reports.** Select **Reports->New Report**. The **New Report** page appears.
- **Creating New Reports from the Manage Reports Page.** Select **Reports->Manage Reports**. The **Manage Reports** page appears. Click **New**. The **New Report** section appears.
- **Editing Reports.** Select **Reports->Manage Reports**. The **Manage Reports** page appears. Select the report that you want to edit, and click **Edit**. The **Edit Report** section appears.
- **Copying Reports.** Select **Reports->Manage Reports**. The **Manage Reports** page appears. Select the report that you want to copy, and click **Copy**. The **Copy report** section appears.
- **Running Reports in HTML Format.** Select **Reports->Manage Reports**. The **Manage Reports** page appears. Select the report you want to run in HTML format, and select **HTML->[Run Report]**.

- **Running Reports in XML Format.** Select **Reports->Manage Reports**. The **Manage Reports** page appears. Select the report you want to run in XML format, and select **XML->[Run Report]**.
- **Running or Downloading Reports in CSV Format.** Select **Reports->Manage Reports**. The **Manage Reports** page appears. Select the report you want to run, or download the report in Comma Separated Value (CSV) format, and select **CSV->[Run Report]**.
- **Showing SQL Queries.** Select **Reports->Manage Reports**. The **Manage Reports** page appears. Select the report you for which want to view the SQL details on and select **[Run Report]->Show SQL queries**.
- **Deleting Reports.** Select **Reports->Manage Reports**. The **Manage Reports** page appears. Select the reports to be deleted, and click **Delete**.

Snapshot Comparison

Snapshot Comparisons enable you to compare up to four systems (with the same operating system) to each other or to compare a single system to itself and observe changes over time. Refer to “Snapshot Comparison Reporting” for more information.

The Snapshot Comparison feature provides you with the following option:

To view a snapshot comparison, select **Reports->Snapshot Comparison**. The **Snapshot Comparison** page appears. Select target systems and click **Next**.

Related Procedures

- System Reporting
- Adding a Report
- Editing a Report
- Copying a Report
- Snapshot Comparison Reporting
- PMP Reporting Options

Related Topics

- System License Information Reporting
- Printing a Cluster Collection Report
- Printing an Event Collection Report
- Printing Reports
- Reference Information
- Reporting Views
- User and User Group Reports
- Toolbox Report
- Authorization Report

System Reporting

A generated report provides you with the following:

- Report name
- Associated system collection

Note:



These are not displayed if there is no collection selected to run the report.

- Report run date and time

Reports can be run in the following formats:

- **HTML (Recommended for viewing).** This option displays the report in HTML format.
- **XML.** This option displays the report in XML format.
- **CSV.** This option displays the report in CSV format.

Note:



The default sort order is based on the system name.

Note:



You can click any column heading to sort in ascending or descending order.

Note:



You can also access the **Manage Reports** page from the **Manage** section of the HP Systems Insight Manager (HP SIM) **Home** page, by clicking the **Manage inventory reports** link.

Running an Existing Report in HTML Format

To view a report, HP recommends that you use the HTML format.

To run a report in HTML format:

1. **Reports->Manage Reports.**
2. Select the report you want to view.
3. Under **Preferred format for generated report**, select **HTML (Recommended for viewing)**.
4. Click **Run Report**. The report appears.

The HTML report enables you to **Show SQL queries**. Refer to “Showing SQL” for more information.

Selecting the Sort Order

The Reporting feature enables you to sort the data after it displays in the **Report Results** page.

- **Ascending Order.** Click the column heading you want to sort by once. The data re-queries in ascending alphabetical order.
- **Descending Order.** Click the column heading you want to sort by twice. The data re-queries in descending alphabetical order.

Viewing an Existing Report in XML Format

1. Under **Report Name**, select the report to be viewed.
2. Under **Preferred format for generated report**, select **XML**.
3. Click **Run Report**. The XML report appears.

Viewing an Existing Report in CSV Format

1. **Reports->Manage Reports.**
2. Under **Report Name**, select the report you want to view.
3. Under **Preferred format for generated report**, select **CSV**.
4. Click **Run Report**. If the browser system has no application associated with CSV files, then the CSV file is displayed in the browser window. If you have an application associated with CSV files, then the CSV file is displayed in the specified application.

If you are using Internet Explorer, and an application such as Excel is installed on the browser system and the CSV file extension is associated with that application, the **Save As** dialog box appears. Click **Save**.

5. Name the file, and in the **Save as type** field, select a format in which to save the file from the dropdown list. Click **Save**. The report is saved.

Printing an Existing Report

From the **Report Results** page, select **File->[Print]** from your browser.

Command Line Interface

Use the `mxreport` command to perform this task from the command line interface (CLI). For assistance with this command, refer to the HP-UX or Linux manpage by entering `man mxreport` at the command line. Refer to “Using Command Line Interface Commands” for more information on the command and a link to the manpage.

Related Procedures

- Adding a Report
- Editing a Report
- Copying a Report

Related Topic

- Reporting

Adding a Report

You can save the report configuration for future use or generate a one-time report.

Note:

A report configuration is a customer-defined set of preferences that pulls specified criteria from the database tables and places it in a report in the specified format. The report configurations can be saved and used to run a report at a later date with live data.

You must have full or limited-configuration-rights to create, save, edit, copy, or delete report configurations. In addition, you must have full-configuration-rights to view a license key. Users with no-configuration-rights can only run the authorized report configurations.



You can also create a new report by selecting **Reports->Manage Reports->[New]**.

If Customer 1 with full-configuration-rights generates a report and a private collection, then Customer 2 with full-configuration-rights is allowed to generate a report using the report configuration and private collection that Customer 1 created. Customer 2 is allowed to edit, save, copy, and delete the report configuration but cannot delete the private collection created by Customer 1.

Adding a New Report

1. Select **Reports->New Report**. The **New Report** window appears.
2. Select target systems. Refer to “Creating a Task” for more information.
3. Click **Next**. The **Specify Parameters** section appears.
 - a. In the **Report Name** field, enter a name for the new report.

- b. In the **Select items to show in report** section, select all of the categories or items to include in the report. You can click the  icon to expand a category, and select specific items or click the  icon to collapse a category.
- c. After you have selected all items to include in the report, select one of the following options:
 - **Show all systems in the same table.** This option displays all categories and items selected in the **Select items to show in report** section in the report. The selected categories appear as tables, and the selected data items appear as column headers in the report. All systems appear in the same table.
 - **Show each system in a separate table.** This option displays all categories and items selected in the **Select items to show in report** section in the report. The selected categories appear as tables, and all the selected data items appear as column headers. Each system appears in an individual table.
4. Under **Preferred format for generated report**, select from the following:
 - **HTML (Recommended for viewing).** This option displays the report in HTML format.
 - **XML.** This option displays the report in XML format.
 - **CSV.** This option displays the report in CSV format.
5. To save the report configuration, click **Save Report**. If the report already exists, the **overwrite report** message appears. Click **Cancel** if you do not want to overwrite the existing report.
6. Click **Run Report**.

The new report appears, providing you with the following:

- Show SQL Queries

Selecting the Sort Order

The Reporting feature enables you to sort the data when it displays on the **Report Results** page.

- **Ascending Order.** Click the column heading you want to sort by once. The data re-queries in ascending alphabetical order.
- **Descending Order.** Click the column heading you want to sort by twice. The data re-queries in descending alphabetical order.

Printing the Report

On the **Report Results** page, select **File->[Print]** from your browser.

Command Line Interface

Use the **mxreport** command to perform this task from the command line interface (CLI). For assistance with this command, refer to the HP-UX or Linux manpage by entering **man mxreport**

at the command line. Refer to “Using Command Line Interface Commands” for more information on the command and a link to the manpage.

Related Procedures

- System Reporting
- Editing a Report
- Copying a Report

Related Topic

- Reporting

Editing a Report

HP Systems Insight Manager (HP SIM) enables you to edit existing report configurations. You can save these updated report configurations over the existing report configuration, or you can save it as a new report configuration.

Note:



You must have full- or limited-configuration-rights to create, save, edit, copy, or delete report configurations. In addition, you must have full-configuration-rights to view a license key. Users with no configuration rights cannot edit the report configurations.

You can also access the **Manage Reports** page from the HP SIM **Home** page, **Manage** section by clicking the **Manage inventory reports** link.

To edit an existing report:

1. Select **Reports->Manage Reports**. The **Manage Reports** window appears.
2. Select the report to edit, and click **Edit**. The **Edit Report** section displays.
3. Select target systems. Refer to “Creating a Task” for more information.
4. Click **Next**. The **Specify Parameters** section appears.
 - a. In the **Select items to show in report** section, select all of the categories or items to be included in the report. You can click the **+** icon to expand a category and select specific items, and then click the **-** icon to collapse a category.
 - b. When you have selected all items to include in the report, select one of the following options:
 - **Show all systems in the same table.** This option displays all categories and items selected in the **Select items to show in report** section in the report. The selected categories appear as tables, and the selected data items appear as column headers in the report. All systems appear in the same table.
 - **Show each system in a separate table.** This option displays all categories and items selected in the **Select items to show in report** section in the report. The

selected categories appear as tables, and all the selected data items appear as column headers. Each system displays in an individual table.

5. Under **Format for current run of generated report (format not saved with report):**, select from the following:
 - **HTML (Recommended for viewing)**. This option displays the report in HTML format.
 - **XML**. This option displays the report in XML format.
 - **CSV**. This option displays the report in CSV format.
6. To save over the existing report configuration, click **Save Report**.

Note: To save an existing report as a report with a new name, enter a new report name in the **Report Name** field, and click **Save Report**. The new report is saved and added to the report list on the **Manage Reports** page.

A dialog box appears asking you to confirm your intention to save the report. Click **OK** to save, or click **Cancel** to abort. If the report already exists, the **overwrite report** message appears. Click **Cancel** if you do not want to overwrite the existing report.
7. To view the report, click **Run Report**. You can click **Previous** to return to the target selection page. You can click **Cancel**, to abort the report creation process.

Command Line Interface

Use the `mxreport` command to perform this task from the command line interface (CLI). For assistance with this command, refer to the HP-UX or Linux manpage by entering `man mxreport` at the command line. Refer to “Using Command Line Interface Commands” for more information on the command and a link to the manpage.

Related Procedures

- Adding a Report
- Showing SQL
- System Reporting

Related Topic

- Reporting

Copying a Report

HP Systems Insight Manager (HP SIM) enables you to copy report configurations from an existing report configuration. You can edit the newly copied configurations to create a new report.

Note:



You must be signed into HP SIM with full or limited-configuration-rights to copy report configurations. If you are not signed in with full or limited-configuration-rights, the copy option is not available.

Note:



You can also access the **Manage Reports** page from the **Manage** section of the HP SIM **Home** page by clicking the **Manage inventory reports** link.

To copy a report configuration:

1. Select **Reports->Manage Reports**. The **Manage Reports** window appears.
2. Select the report to copy and click **Copy**. The **Copy report** section appears.
3. In the **Report Name** field, enter a name for the new report configuration.
4. Click **OK**.

The **Copy report** section closes, and the copied report configuration appears in the **Manage Reports** section.

Command Line Interface

Use the **mxreport** command to perform this task from the command line interface (CLI). For assistance with this command, refer to the HP-UX or Linux manpage by entering **man mxreport** at the command line. Refer to "Using Command Line Interface Commands" for more information on the command and a link to the manpage.

Related Procedures

- System Reporting
- Adding a Report
- Editing a Report
- Showing SQL
- Snapshot Comparison Reporting

Related Topic

- Reporting

Showing SQL

You can view the SQL details behind a report. The **SQL Queries** page details all SQL queries that are used to generate the report.

To show the SQL Queries:

1. Select **Reports->Manage Reports**. The **Manage Reports** page appears.
2. Select the report for which you want to see the SQL details.
3. Click the **Show SQL queries** link.

The **SQL Queries** page appears.

Related Procedures

- System Reporting

Related Topic

- Reporting

Reporting Views

Reporting uses the following database views to generate reports.

Database Views

There are several database views that are included with HP Systems Insight Manager (HP SIM). These views can be used to generate reports in HP SIM. The following views are available:

R_ArrayControllers	R_Batteries	R_CellularSysParComplex
R_CellularSysPartition	R_CellularSysParIOChassis	R_CPU
R_DIMMSlots	R_InstalledBoards	R_Inventory
R_lockdownStatus	R_LogicalDisks	R_NetworkInterface
R_OperatingSystem	R_PhysicalDisks	R_PowerSupply
R_Process	R_Racks	R_Software
R_devicelicenseInfo	R_StorageDeviceInventory	R_StorageDeviceControllers
R_StorageHostBusAdapters	R_StoragePorts	R_StorageLogicalUnits
R_StorageDeviceCapacity	R_UnixOSDetails	R_UnixLogicalMemory
R_UnixIODevices	R_UnixIPRoute	R_HPUXFileSystem
R_HPUXVolumeGroup	R_HPUXLogicalVolume	R_HPUXLogicalVolume
R_HPUXNetworkDetails	R_HPUXKernelParam	R_HPUXSoftwareBundle
R_HPUXSoftwareProduct		

R_ArrayControllers

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
BoardName	Board name

Column Name	Description
Model	Controller model
Version	Controller Product Revision number
FirmwareRev	Board firmware revision
SerialNumber	Controller Serial number
SlotNumber	Slot number in the system
SnapshotID	Snapshot ID
Tag	Tag

R_Batteries

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
SerialNumber	Serial number
AssetNumber	Asset tag number
SnapshotID	Snapshot ID
Tag	Tag

R_CellularSysParComplex

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
ComplexName	Complex name
ComputeCabinets	Number of compute cabinets in the complex
IOCabinets	Number of IOX cabinets in the complex
SnapshotID	SnapshotID

R_CellularSysPartition

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
PartitionName	Partition name
IPAddress	IP address
TotalCPUCore	Number of CPUs in the partition
InstalledCells	Number of installed cells in the partition
PoweredonCells	Number of powered on cells in the partition
CoreCell	Index to cpqSeCellTablePtr for core cell in the partition

Column Name	Description
CoreCellCabinet	Index to cpqSeCellTablePtr for core cell in the cabinet
HasInterleaveMemory	When set, indicates that there is an interleaved memory configured in the partition
SnapshotID	SnapshotID

R_CellularSysParIOChassis

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
PartitionName	Partition name
CabinetNumber	Represents the cabinet that the I/O chassis belongs to
IOBayNumber	Indicates the bay in the cabinet where the I/O chassis resides
IOChassisNumber	The I/O chassis number that is unique across the bay
SnapshotID	SnapshotID

R_CPU

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
CPUType	Type of CPU
CPU Speed	CPU speed
SlotNumber	Slot number in the system
SnapshotID	Snapshot ID
FirmwareID	Processor firmware ID
ProcessorLoad	Processor load
ProcessorAllocated	Processor status: 1=Allocated; 0=Not allocated
Location	Location for 64-bit Intel® platform systems (This field is blank for all other systems)
CellNumber	Cell number
ArchitectureRevision	Architecture revision
FirmwareRevision	Firmware revision
DataWidth	Data width

R_DIMMSlots

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
FormFactor	Type of memory module installed
MemorySize	Memory size in kilobytes
PartNumber	Memory modules manufacturer part number
SerialNumber	Memory modules serial number
SlotNumber	Slot number in the system
MemoryType	Memory type
MemoryTech	Technology type of memory module installed
Location	Location for 64-bit Intel® platform systems (This field is blank for all other systems)
SnapshotID	Snapshot ID
LocationID	Location ID
Description	Description
BankLabel	Bank label
Tag	Tag

R_InstalledBoards

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
BoardName	Board name (for example, PCI SCSI controller, and so on)
BoardModel	Board model
BoardRevision	Board revision
BoardFirmware	Board firmware
BoardSerial	Board serial number
Slot	Slot number in the system
SnapshotID	Snapshot ID
Location	Location for 64-bit Intel® platform systems (This field is blank for all other systems)
Tag	Tag

R_Inventory

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system

Column Name	Description
ProductName	Product name
ProductID	Product ID
MemorySize	Memory size
ROMVersion	ROM version
SerialNumber	Serial number
AssetTag	Asset tag
OSName	Operating System name
IPAddress	IP address
IPLongValue	IP address in decimal value
OSVendor	Operating system vendor
SnapshotID	Snapshot ID
DeviceOwner	Owner of the system
Location	Location of the system
ProductType	Type of system (for example, server, client, workstation, and so on)
DeviceStatus	Hardware status of the system
DeviceBootTime	System Boot Up Time
ProductSubType	Product subtype
ProductTypeStr	Product type
ServerRole	Server role
IPXAddress	IPX address

R_lockdownStatus

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
LastScanName	Name of last vulnerability scan
LastScanDate	Date of last vulnerability scan
LastVulChk	Vulnerability DAT file used in last scan
Critical	Number of Critical vulnerabilities found in the last scan
Major	Number of Major vulnerabilities found in the last scan
Minor	Number of Minor vulnerabilities found in the last scan
LPatchDate	Date and time of last patch event
PatchRqd	Number of patches required (total)
PatchMiss	Number of patches not included (total)

Column Name	Description
Warning	Number of vulnerability Warnings found in the last scan
SnapshotID	SnapshotID

R_LogicalDisks

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
Description	Which logical drive (for example, c: [FAT])
SizeMB	Size of the logical drive in megabytes
UsedMB	Size of used space in megabytes
UsedPercent	Percentage of the used space
SnapshotID	Snapshot ID

R_NetworkInterface

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
Description	Description
MacAddress	MAC address
IPAddress	IP address
InputErrors	Input errors
OutputErrors	Output errors
Speed	Interface speed (bits/s)
Duplex	Adapter Duplex state
FullDuplex	Flag indicating that the adapter is operating in full duplex mode
InterfaceName	Interface name
SubnetMask	Subnet mask
BroadcastAddress	Broadcast address
InterfaceState	Status information to indicate whether the logical system is enabled (3), disabled (4), some other (1), or unknown (2) state
DHCPEnabled	Indicates whether DHCP is enabled
IPLongValue	IP address in decimal value
SnapshotID	Snapshot ID
OperationalStatus	Operational status
ProtocolType	Protocol type
MaxDataSize	Maximum data size

Column Name	Description
PortType	Port type

R_OperatingSystem

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
Description	Description of the operating system type
Version	Version number of the operating system
SubDesc	Additional description (for example, Service Pack, Rev information)
OSType	Operating System type (for example, Windows 2000)
SnapshotID	Snapshot ID
OSVendor	Operating system vendor

R_PhysicalDisks

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
DeviceType	System type (for example, SCSI disk)
DriveModel	Drive model
DriveSize	Drive size
DriveFirmware	Drive firmware
TransferMode	Mode of transfer for ATA drives
DriveSerial	Drive serial number
DriveVendor	Drive vendor (for example, HP)
Slot	Slot number in the system
DriveLoc	The drive number attached to the port
DrivePort	The port
DriveChassis	Populated only for Fibre Channel attached drives and is the name of the chassis that contains the physical disk drive
DriveServiceTime	The total number of hours that a physical drive has been operating under the system driver
HardReadErrors	The number of read errors that have occurred on a drive that could not be recovered by the Error Correction Code (ECC) algorithm of the physical drive or through retries
HardWriteErrors	The number of write errors that could not be recovered by a physical drive

Column Name	Description
DeviceID	Device ID
SnapshotID	Snapshot ID

R_PowerSupply

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
DeviceID	System ID
ModelName	Model name
SerialNumber	Serial number
FirmwareRev	Firmware revision
ConditionVal	Condition value
MaxCapacity	Maximum capacity in watts
UsedCapacity	Used capacity in watts
RedundancyState	Redundancy state of the power supply
Status	Status of the fault tolerant power supply system
Condition	Condition of this power supply
SnapshotID	Snapshot ID
Description	Description

R_Racks

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
RackName	Name of the rack
EnclosureName	Name of the enclosure
Name	Name
SerialNumber	Serial number
Model	Model name
Type	Type
SlotNumber	Slot number
SnapshotID	Snapshot ID

R_Software

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system

Column Name	Description
SnapshotID	Snapshot ID
Description	Software description (for example, Server Agent Service, or Storage Agent Service)
Version	Version number
Executable	Name of the executable
TypeValue	Type value
Status	Software status
Date_	Date the software item
Type	Type of software (for example, agent, application, or driver)

R_deviceLicenseInfo

Column Name	Description
deviceKey	System key
numberLicPurchased	The number of licenses purchased for this key
numberLicUsed	Actual number of licenses in use for this particular license key and system
keyVer	The version of the key in use
Lickey	The key the customer has entered (This column can be blank if you restrict the Integrated Lights-Out (iLO) response to HP SIM requests for license information. This column is not displayed if you do not have permission to view license keys.)
licType	The type of license on the system
licDate	The date the license was applied
productName	The name of the product
productVer	The version of the product; can be blank
expirationDate	The date the product expires
collectDate	The date the collection last took place by HP SIM
DeviceName	Name of system associated with system key
licStatus	License status
SnapShotID	SnapShotID

R_StorageDeviceInventory

Column Name	Description
DeviceKey	System key
DeviceName	Unique name for the system
ControllerName	Name of the controller
WorldWideName	World wide name (WWN) or IP address

Column Name	Description
Vendor	The name of the product supplier
Model	Commonly used product name
ProductRevision	Product version information
FirmwareVersion	Version info related to the software
SerialNumber	Product identification such as serial number
Status	System status
PortCount	The total number of ports on this system
PortUtilized	The number of ports on this system that have something connected
SnapshotID	Snapshot ID

R_StorageDeviceControllers

Column Name	Description
DeviceKey	System key
DeviceName	Unique name for the storage array
ControllerName	Friendly name for the controller
WorldWideName	WWN
Vendor	Vendor
Model	Model
ProductRevision	Product version information
FirmwareVersion	Version info related to the software
SerialNumber	Product identification such as serial number
Status	The controller status
PortCount	The total number of ports on this system
PortUtilized	The number of ports on this system that have something connected
SnapshotID	Snapshot ID

R_StorageHostBusAdapters

Column Name	Description
DeviceKey	System key
DeviceName	Name of the host
HBAName	Friendly name of the Host Bus Adapter (HBA)
WorldWideName	Node WWN of HBA
Vendor	Vendor
Model	Model of the HBA
Status	Status of the HBA
ProductRevision	Product version information

Column Name	Description
DriverVersion	Version of the driver for the HBA
FirmwareVersion	Firmware version of the HBA
FCode_BIOSVersion	FCode/Bios version of the HBA
SerialNumber	Product identification such as serial number
PortCount	The total number of ports on this system
PortUtilized	The number of ports on this system being used
SnapshotID	Snapshot ID

R_StoragePorts

Column Name	Description
DeviceKey	System key
DeviceName	Name of the SAN host, interconnect system, or storage system
PortName	Friendly name of the port
Number	Port number
WorldWideName	WWN of HBA
ControllerHBAName	The name of the parent (For ports on host system, this would be the HBA)
Status	The status of the port
Type	FC-GS port type
Speed	The speed of the established link in bits per second (bps)
MaxSpeed	The maximum speed of the port in bits per second (bps)
SnapshotID	Snapshot ID

R_StorageLogicalUnits

Column Name	Description
DeviceKey	System key
DeviceName	Unique name for the storage system
LUNName	Friendly name of the Logical Unit Number (LUN)
ID	VPD
Status	The status of the LUN
ExtentStatus	Additional status information on the LUN
LUNSize	The capacity of the LUN in bytes
RAIDLevel	Use heuristic based on StorageSetting qualifier to determine the RAID level
StoragePool	The name of the storage pool from which this LUN was carved

Column Name	Description
SnapshotID	Snapshot ID

R_StorageDeviceCapacity

Column Name	Description
DeviceKey	System key
DeviceName	Name of the storage system
ID	Unique ID of storage system
rawcapacity	The total capacity of a storage array in bytes
unallocated	The amount of space on the array that has not been carried into LUNs
carved	The total amount of space used in creating LUNs (If LUN is mirrored, this is the total space used by the LUN and not the space usable by the initiator.)
presented	The amount of usable bytes that have been assigned to ports
unpresented	The number of usable bytes that have been carved into LUNs, but are not assigned to a port
overhead	The number of overhead bytes to create redundancy
snapshotId	Snapshot ID

R_Process

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
ID	ID
Name	Name of the process
State	Process state
Priority	Process priority
SnapshotID	Snapshot ID

R_UnixOSDetails

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
OSName	Name of the operating system
OSVersion	Operating system version
Capability	Operating system capability

Column Name	Description
SystemUptime	System boot up time
NumUsers	Number of users
NumProcesses	Number of processes
MaxProcesses	Max processes
TimeZone	System Date Time
Snapshot ID	Snapshot ID

R_UnixLogicalMemory

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
SwapSpaceName	Swap space name
SwapType	Swap type
SwapSpaceSize	Swap space size
SwapSpaceMinSize	Swap space minimum size
SwapSpaceMaxSize	Swap space maximum size
SwapSpaceReservedSize	Swap space reserved size
SnapshotID	Snapshot ID

R_UnixIODevices

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
DeviceType	System type
DeviceDescription	System description
DeviceIdentifier	System identifier
DeviceStatus	System status
DeviceErrors	System errors
HardwarePath	Hardware path
HardwareType	Hardware type
DeviceClass	System class
AssociatedDriver	System driver
SnapshotID	Snapshot ID

R_UnixIPRoute

Column Name	Description
DeviceKey	System key

Column Name	Description
DeviceName	Name of the system
RouteDestination	Route destination
RouteMask	Route mask
RouteGateway	Route gateway
SnapshotID	Snapshot ID

R_UnixSensors

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
SensorName	Sensor Name
SensorID	Sensor ID
SensorType	Sensor Type
SnapshotID	Snapshot ID

R_HPUXFileSystem

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
MountPointName	Mount point name
MountSpecialDeviceName	Mount special system name
RemoteMountPointName	Remote mount point name
FileSystemType	File system type
FileSystemAccess	File system access
FileSystemBootable	File system bootable
TotalNodes	Total inodes
FreeNodes	Free inodes
DataCapacity	Data capacity
FreeCapacity	Free capacity
MinFreeSpace	Minimum free space
SnapshotID	Snapshot ID

R_HPUXVolumeGroup

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
VolumeGroupName	Volume group name

Column Name	Description
AccessPermission	Access permission
Status	Status
ExtentSize	Physical extent size
Capacity	Volume group capacity
Allocation	Volume group allocated
FreeSpace	Free space
MaxNumPhysicalVol	Maximum number of physical volume
MaxNumPhysicalExtent	Maximum number of physical extent
NumDefinedPhysicalVol	Number of defined physical volume
NumActivePhysicalVol	Number of active physical volumes
MaxNumLogicalVol	Max number of logical volumes
SnapshotID	Snapshot ID

R_HPUXLogicalVolume

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
LogicalVolName	Logical volume name
AccessPermission	Access permission
Status	Logical volume status
ExtentSize	Logical extent size
Capacity	Logical volume capacity
SchedulePolicy	Schedule policy
AllocationPolicy	Allocation policy
SnapshotID	Snapshot ID

R_HPUXPhysicalVolume

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
PhysicalVolName	Physical volume name
Status	Physical volume status
ExtentSize	Physical extent size
Capacity	Physical volume capacity
AllocatedPhysicalExtent	Allocated physical extent
FreePhysicalExtent	Free physical extent
SnapshotID	Snapshot ID

R_HPUXNetworkDetails

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
DomainName	Domain name
Search	Search list
ServerIPAddress	Server IP address
ServerType	Server type: Unknown (0), Other (1), None (2), Master Server (3), Slave Server (4)
ServerWaitFlag	Server wait flag
ServerAddress	Server address
SnapshotID	Snapshot ID

R_HPUXKernelParam

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
ParameterName	Parameter name
ParameterValue	Parameter value
SnapshotID	Snapshot ID

R_HPUXSoftwareBundle

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
BundleName	Bundle name
VendorTag	Vendor tag
Architecture	Architecture
Revision	Revision
Caption	Caption
ModificationTime	Modification time
Size_	Size
LayoutVersion	Layout version
OSName	Operating system name
OSRelease	Operating release
IsPatch	IsPatch
InstallSource	Install source
InstallDate	Install date

Column Name	Description
SnapshotID	Snapshot ID

R_HPUXSoftwareProduct

Column Name	Description
DeviceKey	System key
DeviceName	Name of the system
Specification	Product software specification
ProductName	Product name
Architecture	Architecture
Revision	Revision
VendorTag	Vendor tag
Caption	Product caption
ModificationTime	Modification time
Size_	Size
OSName	Operating system name
OSRelease	Operating system release
IsPatch	IS patch
InstallSource	Install source
InstallDate	Install date
SnapshotID	Snapshot ID

Related Topics

- Reporting
- Snapshot Comparison Reporting

Snapshot Comparison Reporting

Snapshot Comparisons enable you to compare up to four systems (with the same operating system) to each other or to compare a single system to itself and observe changes over time. To perform historical trend analysis for a single system, such as compare snapshot data, you must have already collected at least two sets of snapshot data (by way of **Options->Data Collection**) for that system and select **Append new data set (for historical trend analysis)** in the **Step 2: Specify How to Save Data** page.

To run a snapshot comparison:

1. Select **Reports->Snapshot Comparison**. The **Snapshot Comparison** window appears.
2. Select target systems. Refer to "Creating a Task" for more information.
3. Click **Next**. You can click **Previous** to return to the **Target Selection** page.

Select between two and four snapshots for the systems from the **Select Snapshots** page.

Possible warnings include:

- Some system OS types are unknown
- More than one operating system type is selected
- Only one operating system type comparison is supported
- If one target is selected, this target must have at least two snapshots. You must select between two and four snapshots to compare.
- If more than one target is selected, you can select one snapshot for each system.

The target systems selected should be of the same operating system for the snapshot comparison feature to work.

4. Click **Next**.
5. From the **Select Categories and Baseline** page, select the categories to be included in the snapshot comparison. The **Category Name** column displays the category, and the **Description** column displays a brief description of the category.
6. From the **Select snapshot comparison baseline** section, select an item against which to run the comparison.
7. Click **Run Reports**. You can click **Previous** to return to the **Select Snapshots** page.
8. To view the report, click **Text Output** under **Click the link to view the text report**.

Related Procedures

- System Reporting
- Adding a Report
- Editing a Report

Related Topic

- Reporting

PMP Reporting Options

Three Performance Management Pack (PMP) reports are available through HP Systems Insight Manager (HP SIM):

Note:



PMP reporting is only available on a Windows system and not HP-UX or Linux.

- **Static Analysis Report.** Displays configuration pertaining to server components: processors, memory, network connections, storage, and host buses.

To access **Static Analysis Report**, select **Reports->Performance Management Pack Reports->Static Analysis Report**.

To access help for this option, go to

https://middle_tier:2381/pmptools/help/StaticAnalysisReport.htm where *middle_tier* is the name or IP address of the server that HP SIM and PMP are installed, or access *PMP directory*\Program Files\HP\Performance Management Pack\PMPTools\htm\help\StaticAnalysisReport.htm where *PMP directory* is the PMP directory on the server where PMP is installed.

- **System Summary Report.** Displays the percentage of time the server remains in a bottleneck state and the overall performance utilization of the server for each of its components, along with the server configuration details.

To access **System Summary Report**, select **Reports->Performance Management Pack Reports->System Summary Report**.

To access help for this option, go to

https://middle_tier:2381/pmptools/help/SystemSummaryReport.htm where *middle_tier* is the name or IP address of the server that HP SIM and PMP are installed, or access *PMP directory*\Program Files\HP\Performance Management Pack\PMPTools\htm\help\SystemSummaryReport.htm where *PMP directory* is the PMP directory on the server where PMP is installed.

- **CSV File Generator.** Displays, in detail, the logged data from the PMP repository for all server components in a .csv file for import into desktop analysis or report tools.

To access **CSV File Generator**, select **Reports->Performance Management Pack Reports->CSV File Generator**.

To access help for this option, go to

https://middle_tier:2381/pmptools/help/CSVFileGenerator.htm where *middle_tier* is the name or IP address of the server that HP SIM and PMP are installed, or access *PMP directory*\Program Files\HP\Performance Management Pack\PMPTools\htm\help\CSVFileGenerator.htm where *PMP directory* is the PMP directory on the server where PMP is installed.

Related Topics

- PMP Tools
- PMP Administrative Options

Administering Systems and Events

Users with full-configuration-rights can administer HP Systems Insight Manager (HP SIM). Administration of HP SIM involves:

- Configuring basic settings using the First Time Wizard
- Configuring and running automatic and manual discovery
- Identifying systems
- Managing hosts and template files
- Managing system types by creating, editing, and deleting SNMP and Desktop Management Interface (DMI) rules
- Setting global and single system protocol settings
- Configuring and running status polling tasks
- Configure automatic event handling by creating and editing tasks, deleting events, and configuring e-mail, modem, event filter, SNMP trap, and status change event settings
- Configuring cluster and system settings
- Running data collection tasks
- Customizing the **Home** page options
- Selecting and maintaining default HP Version Control Repository Manager for advanced searches and tasks like installing software and firmware
- Managing toolboxes
- Managing authorizations
- Managing users
- Monitoring the Audit Log
- Creating, editing, exporting, importing, and synchronizing server certificates
- Creating, deleting, exporting, and importing trusted system certificates
- Setting up managed systems
- Set system properties for multiple systems
- Suspend or resume system monitoring for multiple systems
- Specify HP Version Control Repository Manager
- Running Performance Management Pack (PMP) administrative tools from within HP SIM
- Backing up and restoring the HP SIM database on Windows, HP-UX, and Linux systems
- Configuring security settings
- Modifying identification through System Type Manager
- Manage System Keys

Note:



You must be a user with full-configuration-rights on a system to access the **Options** menu and perform HP SIM administration tasks.

Related Procedures

- Viewing the Audit Log
- Configuring the Audit Log File
- Creating New Users
- Creating New Toolboxes

- Creating New User Groups
- Creating New Authorizations
- Updating Authorizations
- Editing User Accounts and User Groups
- Editing Toolboxes
- Deleting User Accounts and User Groups
- Deleting Toolboxes
- Deleting Authorizations
- User and User Group Reports
- Toolbox Report
- Authorization Report
- Exporting a Server Certificate
- Editing a Server Certificate
- Creating a Server Certificate
- Importing a Server Certificate
- Deleting Trusted Certificates
- Exporting Trusted Certificates
- Importing Trusted Certificates
- Requiring Trusted Certificates
- Configuring Cluster Resource Settings
- Configuring Node Resource Settings
- Creating a Data Collection Task
- Configuring Automatic Discovery
- Adding a System Manually
- Disabling or Enabling a Discovery Task
- Creating a New Discovery Task
- Editing a Discovery Task
- Deleting a Discovery Task
- Running a Discovery Task
- Configuring Discovery General Settings
- Adding Systems in a Hosts File to the Database
- Deleting a Hosts File
- Editing a Hosts File
- Creating a New Hosts File
- Creating a New Discovery Template File
- Editing a Discovery Template
- Deleting a Discovery Template
- Configuring E-mail Settings
- Configuring Modem Settings
- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Managing Event Handling Tasks
- Configuring Event Filters
- Configuring SNMP Traps
- Configuring Status Change Events
- WBEM Indications
- Setting Up Managed Systems
- Version Control Repository
- PMP Administrative Options
- Setting Global Protocols
- Setting Protocols for a System or Groups of Systems
- Setting Protocols for a Single System
- Adding a WMI Mapper Proxy
- Editing a WMI Mapper Proxy
- Deleting a WMI Mapper Proxy

- HP-UX/Linux
- Windows
- Configuring Login Events
- Configuring the System Link
- Configuring Browser Timeout Options
- Hardware Status Polling
- Software Status Polling
- Creating a New STM Rule
- Editing STM Rule
- Deleting STM Rule
- Editing System Properties for Multiple Systems
- Suspending or Resuming System Monitoring for Multiple Systems
- Version Control Repository
- PMP Administrative Options

Related Topics

- Users and Authorizations
- Audit Log
- Server Certificates
- Data Collection
- Discovery and Identification
- Events
- Discovery Filters
- Identification
- Protocols
- WMI Mapper Proxy
- Networking and Security
- About Login
- About Secure Task Execution
- Status Polling
- Manage System Types
- Configuring SSH Bypass Properties

Events

Administering events include the following:

- **Automatic Event Handling.** Enables you to manage automatic event handling tasks, create new automatic event handling tasks, and configure e-mail and modem settings.
 - **Managing Tasks.** Enables you to view definitions, copy, edit, view task results, disable or enable, or delete existing Automatic Event Handling tasks. You also have the option to create a new Automatic Event Handling task. Select **Options->Events->Automatic Event Handling->Manage Tasks**.
- Refer to “Managing Event Handling Tasks” for more information.
- **Creating a New Task.** Enables you to create a new automatic event handling task. Select **Options->Events->Automatic Event Handling->New Task**.
 - **E-mail Settings.** Enables you to set up the various e-mail settings needed when sending an e-mail because of an event action. There are two ways to access the **E-mail Settings** page:

- Select **Options->Events->Automatic Event Handling->E-mail Settings**.
 - From the HP Systems Insight Manager (HP SIM) introductory page, click **email** in the **DO THIS NOW to finish the install** section.
- **Modem Settings.** This feature is available to users with full-configuration-rights only and is available for Windows systems only.

There are two ways to access the **Modem Settings for Paging** page:

- Click **Options->Events->Automatic Event Handling->Modem Settings**.
- From the HP SIM introductory page, click **paging** in the **DO THIS NOW to finish the install** section

- **Clearing Events.** Select **Options->Events->Clear Events**. Select the target events to clear and click **Clear**. Refer to “Clearing Events” for more information.
- **Deleting Events.** Select **Options->Events->Delete Events**. After you have selected the targets and the **Tasks Results** page appears, select the events to delete and click **Delete**. The events are deleted from the database. Refer to “Deleting Events ” for more information.
- **Event Filter Settings.** Select **Options->Events->Event Filter Settings**.

You can access the Automatic Event Handling page to edit or delete an existing rule by clicking **Automatic Event Handling** in the **DO THIS NOW to finish the install** section of the HP SIM introductory page. Refer to “Configuring Event Filters” for more information.

- **SNMP Trap Settings.** Select **Options->Events->SNMP Trap Settings**.

Refer to “Configuring SNMP Traps” for more information.

- **Status Change Event Settings.** Select **Options->Status Change Event Settings**.

Refer to “Configuring Status Change Events” for more information.

- **Subscribing to WBEM Events.** Select **Options->Subscribe to WBEM Events**.

Refer to “Subscribing to WBEM Indications” for more information.

- **Unsubscribing to WBEM Events.** Select **Options->Unsubscribe to WBEM Events**.

Refer to “Unsubscribing to WBEM Indications” for more information.

Related Procedures

- Configuring E-mail Settings
- Configuring Modem Settings
- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Managing Event Handling Tasks
- Configuring Event Filters
- Configuring SNMP Traps
- Configuring Status Change Events
- Deleting Events
- Clearing Events

Related Topics

- About Administering Events
- Managing Event Handling Tasks

- Creating a Paging Task Based on E-mail Notification
- Examples of E-mail Pages
- Creating a Paging Task Based on E-mail Notification

About Administering Events

Administering events include the following:

- Automatic Event Handling
- Delete Events
- Event Filter Settings
- SNMP Trap Settings
- Status Change Event Settings

Automatic Event Handling

Automatic Event Handling enables you to define an action that HP Systems Insight Manager (HP SIM) performs when an event is received. Users who want to access this feature require full-configuration-rights.

Four options are available under Automatic Event Handling:

- **New Task.** Used to create new Automatic Event Handling tasks.
- **Manage Tasks.** Used to manage existing Automatic Event Handling tasks.
- **Configure e-mail settings.** Used to send e-mails to alert users of problems. Because mail systems differ in their requirements, check with your e-mail administrator to verify whether you need the following information:
 - SMTP Host name of the outgoing mail server, such as *mail.company.com*. This server receives the mail messages from HP SIM and begins routing it to the recipient.
 - The name of the management server e-mail address. This address appears in the From field of any e-mail sent from HP SIM. The user can be a system name. Enter the full domain address in the form, *server@domain.com*, as the sender.

Note:



Some e-mail systems require a valid From user before they accept the message. HP suggests that a valid e-mail account be used for this purpose.

- **Configure modem settings (Windows only).** This feature is available to users with full-configuration-rights.

Set up a modem to use for alphanumeric paging. Before you can send a page from the HP SIM server, set up the modem on the server. Be sure you know the COM port used by the modem to send the page to set up the modem in HP SIM.

Access the Automatic Event Handling page to edit or delete an existing rule by clicking **Automatic Event Handling** in the **DO THIS NOW to finish the install** section of the HP SIM introductory page.

Delete Events

This task is used to delete tasks from the database.

Note:



Events can be deleted from the event view page. Refer to “Customizing Event Collections” for more information.

Event Filter Settings

Event filtering is a way to filter SNMP traps you receive from discovered systems. The default setting is to accept all registered SNMP traps from all discovered systems. You can specify the severity of the traps you want to see and use the IP address ranges to create a subset of systems whose traps you can receive or ignore. For example, you can use event filtering to ignore informational traps. This feature is available to users with full-configuration-rights. Refer to “Managing MIBs” for information on compiling MIBs.

Options for Filtering Events

Events are registered or unregistered. Registered events are SNMP traps that are recognized by HP SIM from systems that have been discovered. Unregistered events are traps from systems that were discovered but whose system information is not part of the HP SIM MIBs database. Only registered events have a severity level. Refer to “Event Severity Types” for information on event severity types.

You can specify IP ranges for accepting or discarding traps. Enter one system or range per line, or separate the ranges and systems with a semicolon (;).

You can also filter traps using SNMP Extensions.

SNMP Trap Settings

This feature is available to users with full-configuration-rights and is used to view or edit trap details for a registered MIB.

SNMP traps enable you to tailor trap messages to your specific network needs. Trap messages can be cryptic, poorly written, and incomprehensible. You can modify the MIB information in the database representation. You can also modify a `.cfg` file of the MIB. HP recommends that you never modify an actual MIB. Refer to “Editing a MIB” for more information on editing MIBs.

Status Change Event Settings

This page is used to configure the settings for sending status change events for systems when hardware status changes.

Related Procedures

- Configuring E-mail Settings
- Configuring Modem Settings
- Creating an Automatic Event Handling Task with an Existing Event Collection
- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Managing Event Handling Tasks
- Configuring Event Filters
- Configuring SNMP Traps
- Configuring Status Change Events

Related Topics

- Events
- Examples of E-mail Pages
- Creating a Paging Task Based on E-mail Notification

Creating a New Automatic Event Handling Task with Specified Events and System Attributes

Create an automatic event handling task with an existing event collection or with event and system attributes that you can specify.

Creating an automatic event handling task

To create a new task for handling incoming events automatically, select **Options->Events->Automatic Event Handling->New Task**.

Select one of the following options:

- **with an existing event collection.** There are five steps to complete this task.
 - Select task name
 - Select existing event collection
 - Select actions
 - Select time filter
 - Review summary
- **with event and system attributes that I will specify.** There are six steps to complete this task.
 - Select task name
 - Select events
 - Select systems
 - Select actions

- Select time filter
- Review summary

Related Procedures

- Configuring E-mail Settings
- Configuring Modem Settings
- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Creating an Automatic Event Handling Task with an Existing Event Collection
- Managing Event Handling Tasks
- Configuring Event Filters
- Configuring SNMP Traps
- Configuring Status Change Events

Related Topics

- Events
- About Administering Events
- Examples of E-mail Pages

Managing Event Handling Tasks

Perform the following procedures to create, edit, copy, view definition, view task results, enable/disable, or delete automatic event handling tasks.

Caution:



If you delete an automatic event handling task, the task is permanently deleted and cannot be restored.

To manage automatic event handling tasks:

1. Select **Options->Events->Automatic Event Handling->Manage Task**. The **Automatic Event Handling - Manage Tasks** page appears.
2. Select a task.
3. Click one of the following:
 - Click **New** to create a new automatic event handling task. Refer to “Creating an Automatic Event Handling Task with Selected Event and System Attributes” for more information.
 - Click **Edit** to edit the task. The edit wizard appears, which is similar to the page for creating a new automatic event handling task, but the fields are pre-populated with the current settings for the task. An additional field is available to reassign the task owner. Refer to “Editing Automatic Event Handling Tasks” for more information.
 - Click **Copy** to replicate the configuration details of an existing task. A **Copy Task** page appears below the task list. Specify a new task name in the **Task name** box. Click **OK**,

and a new and separate task is created. Refer to “Copying Automatic Event Handling Tasks” for more information.

- Click **View Definition** to view the task. The entire configuration for the selected task such as Task name, event, system criteria, Action(s), Modem settings, and E-mail settings appear. Refer to “Viewing Task Definitions” for more information.
- Click **Task Results** to view the task result details for a selected task below the list. Refer to “Viewing Event Task Results” for more information.
- Click **Disable** to disable a task. Refer to “Enabling or Disabling Automatic Event Handling Tasks” for more information.
- Click **Delete** to delete the task. A confirmation box appears. Click **OK** to delete, or click **Cancel** to cancel the deletion. Refer to “Deleting Events ” for more information.

Related Procedures

- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Creating an Automatic Event Handling Task with an Existing Event Collection
- Editing Automatic Event Handling Tasks
- Copying Automatic Event Handling Tasks
- Viewing Task Definitions
- Viewing Event Task Results
- Enabling or Disabling Automatic Event Handling Tasks
- Deleting Events
- Configuring E-mail Settings
- Configuring Modem Settings

Related Topics

- Events
- About Administering Events
- Examples of E-mail Pages

Creating an Automatic Event Handling Task with Selected Event and System Attributes

Perform the following procedure to create a new automatic event handling task to define a response to a specific event.

Note:



There is a selection limit of 100 servers for automatic event handling tasks.

Note:



If you create an automatic event handling task using the **with event and system attributes that I will specify** option and use the `mxtask -if` command to create an XML file that can be used to create another task, the task and collection that are associated with the task are placed in the XML file. If you delete the task, the collection is deleted along with the task. Therefore, the XML file can no longer be used to create a new task with the collection that is referenced in the XML file. Refer to the *HP Systems Insight Manager Command Line Interface Reference Guide* for more information.

To define a new task:

1. Select **Options->Events->Automatic Event Handling->New Task**. The **Automatic Event Handling - New Task** page appears.
2. Select **with event and system attributes that I will specify**.
3. There are six steps to complete to define a new task. Under **Step 1 of 5, Select name** is selected. Enter a name for the task in the **Task name** field.
4. Click **Next**. The step 2, **Select existing event collection** page appears.
5. Select the event search criteria for defining the task:
 - List criteria
 - Comparison option
 - Value for the criteria or comparison options selected

To add additional search criteria, click **Add**.

Refer to “Performing an Advanced Search for Events” for more information on event searches.
6. When you have entered the information, click **Next** to continue with the next step or **Previous** to return to the previous step. The step 3, **Select systems** appears .
7. Select the system criteria for defining the task.from the dropdown lists:
 - List criteria
 - Comparison option
 - Value for the criteria or comparison options selected
8. To add additional criteria, click **Add**. Refer to “Performing an Advanced Search for Events”.
9. When you have entered the information, click **Next** to continue with the next step or click **Previous** to return to the previous step. Step 4, **Select actions** page appears.
10. Select from the following:
 - Send page (Windows only)

Add users to be paged from the dropdown list of users by clicking >>. Click << to remove users from the list of users to be paged. The pager number for an HP Systems Insight Manager (HP SIM) user is set on the **Users and Authorizations** page. Refer to “Creating New Users” for more information. If a user name in the **Users** list is inactive, the pager information for the user has not been configured. You can add the user to the list of users to be paged, but pager messages are not sent to this user until the pager information is provided on the **Users and Authorizations** page.

- Send e-mail

In the **To** field, enter the list of e-mail addresses that should receive the notification, separating each entry with a comma.

In the **CC** field, enter any e-mail address that should receive a copy of the e-mail, separating each entry with a comma.

In the **Subject** field, enter a note describing the subject of the e-mail.

In the **Message Format** field, select from the following formats based on the encoding preference of the recipient:

- Standard**. A default message format that sends a text e-mail message to the recipients
- Pager/SMS**. An e-mail message formatted with the same information and format as a pager message is sent to the recipients
- HTML**. An e-mail message that looks like the **HTML Event Details** page is sent to the recipients

In the **Encoding** field, select from the following formats:

- Western European (ISO-8859-1)**
- Unicode (UTF-8)**
- Japanese (ISO-2022-JP)**
- Japanese (Shift_JIS)**
- Japanese (EUC-JP)**

- Run custom command

Select a custom command from the **Name** dropdown list. Custom commands are created under the **Tools->Custom Commands->New Custom Command** option. Refer to “Creating a New Custom Command” for more information.

- Assign

Enter the name of the person to whom to assign the task. The event is assigned to this user when received.

- Forward as SNMP trap

Enter a system name or IP address in the **Name or IP** text field, and click >> to add it to the **Trap recipients** box.

Click **Delete** if you want to delete a recipient after first highlighting the name in the **Trap recipients** box. Use the up and down arrows to scroll to the recipient to delete.

- Write to system log

On Windows NT and Windows XP systems, the event details are written to the Application Log, and the **Source** column of the Event Log is listed as **HP SIM** for the logged event. On Linux and HP-UX systems, the event details are logged to the system log, which is usually located in the file `/var/log/messages` on Linux and in `/var/adm/sysLog/syslog.log` on HP-UX.

- Clear event

Received events are cleared based on the criteria selected when task executes.

11. After you have made your selections, click **Next** to continue with the next step or **Previous** to return to the previous step. The step 5, **Select time filter** appears.
12. Select the box if you want to use time filters, and select an option from the dropdown list.
 - a. Click **Manage Filters** if you want to set user defined filters. Refer to “Applying a Time Filter” for more information.
 - b. Select the **View time filter** box. A time filter popup window appears, showing the times selected.

If the **Use time filter** checkbox is not selected, actions are triggered whenever the events matching the selected criteria are received.

If the **Use time filter** checkbox is selected, actions are triggered **only** when they occur during the days and times specified by the selected time filter.
 - c. When you have entered the information, click **Next** to continue with the next step or **Previous** to return to the previous step. Step 6, **Review summary** page appears. The **Task name**, the **events**, **system criteria**, and **Action(s)** information are displayed. If a paging or e-mail option was selected, the modem and e-mail settings are displayed, along with buttons to change the settings.
13. Click **Edit Modem Settings** to edit the modem settings, or click **Edit e-mail Settings** to edit the SMTP settings. Refer to “Configuring Modem Settings” or “Configuring SNMP Traps” for more information.

Note: The event and system search criteria are displayed at the bottom of the page. This information can be extremely complex and long. Therefore, you might need to scroll down to view all of the criteria.

14. Click **Finish** to create the new task, or click **Previous** to go back to the previous step.

Related Procedures

- Creating an Automatic Event Handling Task with an Existing Event Collection
- Managing Event Handling Tasks
- Configuring E-mail Settings
- Configuring Event Filters

- Configuring Modem Settings
- Configuring Status Change Events
- Configuring SNMP Traps
- WBEM Indications

Related Topics

- Events
- About Administering Events
- Creating a New Automatic Event Handling Task with Specified Events and System Attributes
- Examples of E-mail Pages

Creating an Automatic Event Handling Task with an Existing Event Collection

Perform the following procedure to create a new automatic event handling task to define a response to a specific event.

Note:



In previous version of HP Systems Insight Manager (HP SIM), there was a selection limit of 100 servers for automatic event handling tasks. With HP SIM 5.0, there is no longer a limitation.

To define a new task:

1. Select **Options->Events->Automatic Event Handling->New Task**. The **Automatic Event Handling - New Task** page appears.
2. Select **with an existing event collection**. The step 1 **Select name** appears.
3. Enter a name for the task in the **Task name** box.
4. Click **Next**. The step 2, **Select existing event collection** page appears.
5. Select the event collection from the dropdown list. This step enables you to select an event collection and its associated system collection. Click **View** to view a read-only view of the event and system collection criteria. Click **Previous** to return to the previous step, or click **Next** to continue with the next step. The step 3, **Select actions** page appears.
6. Select actions for this task. Select from the following:
 - Send page (Windows only)

Add users to be paged from the dropdown list of users by clicking >>. Click << to remove users from the list of users to be paged. The pager number for an HP SIM user is set on the **Users and Authorizations** page. Refer to "Creating New Users" for more information. If a user name in the **Users** list is inactive, the pager information for the user has not been configured. You can add the user to the list of users to be paged, but pager messages are not sent to this user until the pager information is provided on the **Users and Authorizations** page.

- Send e-mail

In the **To** field, enter the list of e-mail addresses that should receive the notification.

In the **CC** field, enter any e-mail address that should receive a copy of the e-mail, separating each with a comma.

In the **Subject** field, enter a note describing the subject of the e-mail.

In the **Message Format** field, select from the following formats based on the encoding preference of the recipient:

- Standard**. A default message format that sends a text e-mail message to the recipients
- Pager/SMS**. An e-mail message formatted with the same information and format as a pager message is sent to the recipients
- HTML**. An e-mail message that looks like the **HTML Event Details** page is sent to the recipients

In the **Encoding** field, select from the following formats:

- Western European (ISO-8859-1)**
- Unicode (UTF-8)**
- Japanese (ISO-2022-JP)**
- Japanese (Shift_JIS)**
- Japanese (EUC-JP)**

- Run custom command

Select a custom command from the **Name** dropdown list. Custom commands are created under the **Tools->Custom Commands->New Custom Command** option. Refer to "Creating a New Custom Command" for more information.

- Assign

Enter the name of the person to whom to assign the task. The event is assigned to this user when received.

- Forward as SNMP trap

Enter a system name or IP address in the **Name or IP** text field, and click >> to add it to the **Trap recipients** box.

Click **Delete** if you want to delete a recipient after first highlighting the name in the **Trap recipients** box. Use the up and down arrows to scroll to the recipient to delete.

- Write to system log

On Windows NT and Windows XP systems, the event details are written to the Application Log, and the **Source** column of the Event Log is listed as **HP SIM** for the logged event. On Linux and HP-UX systems, the event details are logged to the system log, which is usually

located in the file `/var/log/messages` on Linux and in `/var/adm/sysLog/syslog.log` on HP-UX.

- Clear event

Received events are cleared based on the criteria selected when task executes.

7. After you have made your selections, click **Next** to continue with the next step or **Previous** to return to the previous step. The step 4, **Select time filter** pages appears.
8. Select the **Use time filter** box if you want to use time filters, and select an option from the dropdown list.
 - a. Click **Manage Filters** if you want to set user defined filters. Refer to “Applying a Time Filter” for more information.
 - b. Click **View time filter**. A time filter popup window appears, showing the times selected.

If the **Use time filter** checkbox is not selected, actions are triggered whenever the events matching the selected criteria are received.

If the **Use time filter** checkbox is selected, actions are triggered **only** when they occur during the days and times specified by the selected time filter.
 - c. When you have entered the information, click **Next** to continue with the next step or **Previous** to return to the previous step. The step 5, **Review summary** page appears. The **Task name**, the **selected event collection**, the **events**, **system criteria**, and **Action(s)** information are displayed. If a paging or e-mail option was selected, the modem and e-mail settings are displayed, along with buttons to change the settings.
9. Click **Edit Modem Settings** to edit the modem settings, or click **Edit e-mail Settings** to edit the SMTP settings. Refer to “Configuring Modem Settings” or “Configuring SNMP Traps” for more information.
10. Click **Finish** to create the new task, or click **Previous** to go back to the previous step.

Related Procedures

- Creating a New Automatic Event Handling Task with Specified Events and System Attributes
- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Managing Event Handling Tasks
- Configuring E-mail Settings
- Configuring Event Filters
- Configuring Modem Settings
- Configuring Status Change Events
- Configuring SNMP Traps
- WBEM Indications

Related Topics

- Events
- About Administering Events
- Examples of E-mail Pages

Editing Automatic Event Handling Tasks

1. Select **Options->Events->Automatic Event Handling**. The **Automatic Event Handling - Manage Tasks** page appears.
2. Select the task to edit and click **Edit**. The **Edit task** section appears.
3. To edit the task configuration complete all steps.

Refer to “Creating an Automatic Event Handling Task with an Existing Event Collection ” and “Creating an Automatic Event Handling Task with Selected Event and System Attributes” for more information on each of the steps.

Related Procedures

- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Creating an Automatic Event Handling Task with an Existing Event Collection
- Copying Automatic Event Handling Tasks
- Viewing Task Definitions
- Viewing Event Task Results
- Enabling or Disabling Automatic Event Handling Tasks
- Deleting Events
- Configuring E-mail Settings
- Configuring Modem Settings

Related Topics

- Events
- About Administering Events
- Examples of E-mail Pages

Copying Automatic Event Handling Tasks

Complete the following procedure to replicate the configuration details of an existing task.

To copy tasks:

1. Select **Options->Events->Automatic Event Handling**. The **Automatic Event Handling - Manage Tasks** page appears.
2. Select the task to copy and click **Copy**. The **Copy task** section appears.
3. In the **Task name** field, enter a name for the new task.
4. Click **OK**. The task is copied with a new name and placed in the list of Automatic Event Handling tasks.

Related Procedures

- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Creating an Automatic Event Handling Task with an Existing Event Collection
- Editing Automatic Event Handling Tasks
- Viewing Task Definitions
- Viewing Event Task Results

- Enabling or Disabling Automatic Event Handling Tasks
- Deleting Events
- Configuring E-mail Settings
- Configuring Modem Settings

Related Topics

- Events
- About Administering Events
- Examples of E-mail Pages

Viewing Task Definitions

Complete the following procedure to view the entire task configuration for a selected task. These configuration options were set when creating the task.

1. Select **Options->Events->Automatic Event Handling**. The **Automatic Event Handling - Manage Tasks** page appears.
2. Select a task and click **View Definition**. The **View Definition** section appears displaying the following information:
 - **Task name.** The name given to the task when it was created
 - **Event collection.** The event collection that was selected when the task was created
 - **Events.** The event search criteria set for the task
 - **Systems.** The system collection selected for the task
 - **Action(s).** The actions selected when the task was created, such as, send e-mail and write to system log
 - **E-mail settings.** The e-mail settings set when the task was created

Refer to “Creating an Automatic Event Handling Task with an Existing Event Collection ” and “Creating an Automatic Event Handling Task with Selected Event and System Attributes” for more information on each of the settings.

Related Procedures

- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Creating an Automatic Event Handling Task with an Existing Event Collection
- Editing Automatic Event Handling Tasks
- Copying Automatic Event Handling Tasks
- Viewing Event Task Results
- Enabling or Disabling Automatic Event Handling Tasks
- Deleting Events
- Configuring E-mail Settings
- Configuring Modem Settings

Related Topics

- Events

- About Administering Events
- Examples of E-mail Pages

Viewing Event Task Results

1. Select **Options->Events->Automatic Event Handling**. The **Automatic Event Handling - Manage Tasks** page appears.
2. Select a task to view the task results and click **Task Results**. The **Task details** section appears.
Refer to “Task Results List” for more information on the details displayed.

Related Procedures

- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Creating an Automatic Event Handling Task with an Existing Event Collection
- Editing Automatic Event Handling Tasks
- Copying Automatic Event Handling Tasks
- Viewing Task Definitions
- Enabling or Disabling Automatic Event Handling Tasks
- Deleting Events
- Configuring E-mail Settings
- Configuring Modem Settings

Related Topics

- Events
- About Administering Events
- Examples of E-mail Pages

Enabling or Disabling Automatic Event Handling Tasks

Note:



This option is especially useful for notification tasks imported from Insight Manager 7, which are imported into HP Systems Insight Manager (HP SIM) in a disabled state. You can edit these tasks, verify that the settings are accurate, and then enable the tasks by clicking **Enable**.

Note:



The button label changes depending on if the task is currently enabled or disabled.

1. Select **Options->Events->Automatic Event Handling->Manage Task**. The **Automatic Event Handling - Manage Tasks** page appears.

2. Select a task to enable or disable.
3. If the task is enabled and you want to disable it, click **Disable**, or, if the task is disabled and you want to enable it, click **Enable**.

Related Procedures

- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Creating an Automatic Event Handling Task with an Existing Event Collection
- Editing Automatic Event Handling Tasks
- Copying Automatic Event Handling Tasks
- Viewing Task Definitions
- Viewing Event Task Results
- Deleting Events
- Configuring E-mail Settings
- Configuring Modem Settings

Related Topics

- Events
- About Administering Events
- Examples of E-mail Pages

Configuring E-mail Settings

Perform the following procedure to set the SMTP host and central management server e-mail.

To set SMTP settings for e-mail:

1. Select **Options>Events>Automatic Event Handling>E-mail Settings**. The **E-mail Settings** page appears.
2. Specify the SMTP host in the **SMTP Host** box.
3. Specify the e-mail address that the management server uses when sending e-mail notifications in the **Sender's Email Address** box.
4. To authenticate your SMTP server, select **Server Requires Authentication**.
5. Specify the account name in **Account name** box.
6. Specify the password in the **Password** box.
7. Click **OK** to save changes.

Note:



If the password entered is incorrect, no e-mail notification is sent to that particular recipient.

Related Procedures

- Managing Event Handling Tasks
- Creating a New Automatic Event Handling Task with Specified Events and System Attributes
- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Creating an Automatic Event Handling Task with an Existing Event Collection
- Configuring Event Filters
- Configuring Modem Settings
- Configuring Status Change Events
- Configuring SNMP Traps
- WBEM Indications

Related Topics

- Events
- About Administering Events
- Examples of E-mail Pages
- Creating a Paging Task Based on E-mail Notification

Configuring Modem Settings

Perform the following procedure to specify the COM port used by the modem to send pager messages.

Note:



You can configure modem settings in Windows only.

To set modem settings for paging:

1. Select **Options->Events->Automatic Event Handling->Modem Settings**. The **Modem Settings** page appears.
2. From the **COM port** field, select the appropriate COM port. Refer to your modem documentation for details.
3. Click **OK** to save the setting.

Related Procedures

- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Creating an Automatic Event Handling Task with an Existing Event Collection
- Editing Automatic Event Handling Tasks
- Copying Automatic Event Handling Tasks
- Viewing Task Definitions
- Viewing Event Task Results
- Enabling or Disabling Automatic Event Handling Tasks
- Deleting Events
- Configuring E-mail Settings

Related Topics

- Events
- About Administering Events
- Examples of E-mail Pages

Clearing Events

1. Select **Options->Events->Clear**. The **Clear Events** page appears.
2. Select the target events. Refer “Creating a Task” for more information on selecting targets.
3. Click **Apply**.
4. Click **Run Now** to clear the events immediately and view the **Task Results** page, or click **Schedule** to schedule the deletion. Refer to “Scheduling a Task” for more information on scheduling the task to run.

Note:



When an event is cleared in HP Systems Insight Manager (HP SIM), it is also cleared in HP Storage Essentials.

When an event is cleared in HP Storage Essentials, it is also cleared in HP SIM.

Related Procedures

- Configuring E-mail Settings
- Configuring Modem Settings
- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Managing Event Handling Tasks
- Configuring Event Filters
- Configuring SNMP Traps
- Configuring Status Change Events
- Deleting Events

Related Topics

- Events
- About Administering Events
- Examples of E-mail Pages
- Service Notification Events

Deleting Events

1. Select **Options->Events->Delete**. The **Delete Events** page appears.
2. Select the target events. Refer to “Creating a Task” for more information on selecting targets.
3. Click **Apply**.

4. (Optional) Click **Add Targets** to add additional events to delete, or click **Remove Targets** to remove events from the deletion process.
5. Click **Run Now** to delete the events immediately and view the **Task Results** page, or click **Schedule** to schedule the deletion. Refer to "Scheduling a Task" for more information on scheduling the task to run

Note:



Deleting an event in HP Systems Insight Manager (HP SIM) does not cause the event to be deleted in HP Storage Essentials.

Deleting an event in HP Storage Essentials does not cause the event to be deleted in HP SIM.

Related Procedures

- Configuring E-mail Settings
- Configuring Modem Settings
- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Managing Event Handling Tasks
- Configuring Event Filters
- Configuring SNMP Traps
- Configuring Status Change Events
- Clearing Events

Related Topics

- Events
- About Administering Events
- Examples of E-mail Pages
- Service Notification Events

Configuring Event Filters

Perform the following procedure to specify event filtering settings for registered SNMP traps.

To configure event filtering:

1. Select **Options->Events->Event Filter Settings**. The **Event Filter Settings** page appears.
2. Select **Accept Unregistered Events** to accept unregistered events, or deselect the box to not accept unregistered events.
3. Select **Accept Registered Events with Severity** to accept registered events with a certain severity or multiple severities.
4. Select the severities you want to accept. The available options are Critical, Major, Minor, Warning, and Informational.
5. Enter the IP ranges to accept in the **Accept Traps from Discovered Systems in IP Ranges:** box.

6. Enter IP ranges in the **Discard Traps from Discovered Systems in IP Ranges:** box to discard traps from certain systems (optional).

Note: Enter one system or range per line, and separate the ranges and systems with a semicolon (;). Enter an asterisk (*) to accept or delete traps from all ranges.

7. Click **OK** to accept settings.

Related Procedures

- Managing Event Handling Tasks
- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Configuring E-mail Settings
- Configuring Modem Settings
- Configuring Status Change Events

Related Topic

- Events
- About Administering Events
- Managing MIBs

Configuring SNMP Traps

Perform the following procedure to view and edit user-modifiable attributes associated with SNMP Traps.

To configure SNMP Traps:

1. Select **Options->Events->SNMP Trap Settings**. The **Snm Trap Settings** page appears.
2. Select the MIB name from the **MIB Name** dropdown list.
3. Select the trap name from the **Trap Name** dropdown list. The **Event Type** and **Description** change according to the trap name selected.
4. (Optional) Change the **Event Type**.
5. (Optional) **Edit the Description**.
6. Select **Yes** or **No** in the **Enable Trap Handling** box.
7. Select the category from the **Category** dropdown list.
8. Select the severity from the **Severity** dropdown list. The available options are Informational, Warning, Minor, Major, and Critical.
9. Click **OK** to save the settings.

SNMP Trap Fields

Field Names	Description
MIB Name	Select a MIB name from the dropdown list. All the remaining fields change according to the MIB name selected.
Trap Name	The default trap name is completed when a MIB name is selected in the MIB Name field. However, you can modify it by selecting a different trap name in the dropdown list.
Event Type	The type is a reflective form of the actual trap name. Change the type if it does not adequately describe the system for you.
Description	The description is vendor-supplied. Replace it with more specific instructions, a precise reference source, or a website referral.
Enable Trap Handling	Most traps are enabled. Trap handling gives you control over the volume of messages. Turn off nuisance messages, such as unnecessary informational messages, or repeated trap messages for an event that has not been corrected.
Category	The category lists the HP Systems Insight Manager (HP SIM) category types and Unknown.
Severity	Some vendors use the default Informational for all severity levels. Change the severity to a level that reflects your judgment of the problem. Alternatively, you can change a Major or Critical severity for a trap message that is clearly not a critical situation in your environment. Only you know if this is the case. The only valid options for HP SIM are Critical, Major, Minor, Warning, and Informational.

Related Procedures

- Configuring E-mail Settings
- Configuring Event Filters
- Configuring Modem Settings
- Managing Event Handling Tasks
- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Configuring Status Change Events
- WBEM Indications

Related Topics

- Events
- About Administering Events
- Examples of E-mail Pages
- Managing MIBs

Configuring Status Change Events

Perform the following procedure to configure the sending of status change events for systems when hardware status changes to and from a Critical (unreachable) state only.

To configure status change event settings:

1. Select **Options->Events->Status Change Event Settings**. The **Status Change Event Settings** page appears.
2. Two options are available on this page. Select one or both of the options.
 - **Enable creation of system status change events**. This option causes a system unreachable event to be sent whenever a system cannot be reached by a ping through the Hardware Status Polling task. Enabling this option causes a system reachable event to be created whenever the system is reachable again.
 - **Automatically clear unreachable system status change events when system is reachable**. If this option is enabled, when a system that was previously unreachable starts to respond, the previous unreachable event is marked with a cleared state.
3. Click **OK** to apply changes.

Related Procedures

- Managing Event Handling Tasks
- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Configuring E-mail Settings
- Configuring Event Filters
- Configuring Modem Settings
- Configuring SNMP Traps
- WBEM Indications

Related Topics

- Events
- About Administering Events
- Examples of E-mail Pages

WBEM Indications

HP Systems Insight Manager (HP SIM) enables you to add and remove subscriptions to Web Based Enterprise Management (WBEM) indication events through the graphical user interface (GUI). You can also add and remove subscriptions to WBEM indication events from the command line interface (CLI). If you do not subscribe to WBEM indication events for a system that supports them, any WBEM events that occur will not appear on the Event View Page.

OpenSSH must be installed and set up on the central management server (CMS) with the keys enabled for SSH. Refer to "Installing OpenSSH" for more information.

WBEM events work on HP-UX, Linux, and SMI-S devices (such as storage, switches, and tape libraries). WBEM events for HP-UX and Linux systems require WBEM services 2.0 to be installed on the managed systems. Each managed system must have the correct event provider installed (for

example, the EMS wrapper indication (event) provider on HP-UX). Refer to “Setting Up Managed Systems” for information on installing WBEM services and providers. The `mxwbemsub` command requires root privilege on HP-UX or Linux. OpenSSH is only used when menu tools are executed. If `mxwbemsub` is executed at the command line, it does not require OpenSSH.

To set the port on which WBEM indications are received, edit the `globalsettings.props` file and the `WBEM_indications_Listener_Port` property. The default value for the port is 50004 (`WBEM_indications_Listener_Port=50004`). If this port is unavailable, edit the file and assign a suitable value. If HP SIM is running, stop the service and restart it for the new port to be accessed. If WBEM event subscriptions have been set up with the default port settings, they should be deleted and added again so that the new port is used when WBEM events are sent to the CMS.

You can subscribe and unsubscribe to WBEM indication events. To access these options, select **Options>Events>Subscribe to WBEM Events** and **Options>Events>Unsubscribe to WBEM Events**.

Related Procedure

- Subscribing to WBEM Indications
- Unsubscribing to WBEM Indications

Related Topics

- WBEM Indications
- Creating a Task
- Scheduling a Task
- Task Results List

Subscribing to WBEM Indications

1. Select **Options>Events>Subscribe to WBEM Events**. The **Step 1: Select Target Systems** page appears.
2. Select the target systems and click **Apply**. The **Step 1: Verify Target Systems** page appears.
3. Click **Next**. The **Step 2: Task Confirmation** page appears and provides details about the task that was created in the previous steps.
4. Click **Run Now** to add subscriptions for WBEM events on the target systems. The **Task Results** page appears.

Related Procedure

- Unsubscribing to WBEM Indications

Related Topics

- WBEM Indications
- Creating a Task
- Scheduling a Task
- Task Results List

Unsubscribing to WBEM Indications

1. Select **Options->Events->Unsubscribe to WBEM Events**. The **Step 1: Verify Target Systems** page lists all of the targets with subscriptions to WBEM indication events.
2. If you do not want to delete a target's WBEM indication events subscription, select the checkbox next to the target and click **Remove Targets**.
3. Click **Next**. The **Step 2: Task Confirmation** page is displayed and provides details about the task that was created in the previous steps.
4. Click **Run Now** to remove subscriptions for WBEM indication events on the target systems. The **Task Results** page is displayed.

Instead of clicking **Run Now**, you can click **Schedule** to schedule the task for a later time. Refer to “Scheduling a Task” for more information.

Note:



You can also list subscriptions and move subscriptions to a new destination through the CLI using the `mxwbemsub` command. Refer to “Using Command Line Interface Commands” for more information.

Related Procedure

- Subscribing to WBEM Indications

Related Topics

- WBEM Indications
- Creating a Task
- Scheduling a Task
- Task Results List

Examples of E-mail Pages

There are three types of e-mail pages that can be sent from HP Systems Insight Manager (HP SIM):

- Standard
- Pager/SMS
- HTML

For more information on each type of page, refer to “Creating an Automatic Event Handling Task with Selected Event and System Attributes”.

Example of Standard E-Mail Page

From: Doe, John
Sent: Wednesday, April 28, 2004 5:04 PM
To: Doe, Jane
Cc: Smith, Jim; Jones, Beth
Subject: System A: Storage System side panel is removed (Ver. 3):
Standard E-mail format

Event Name: Storage System side panel is removed (Ver. 3)
Event originator: System A
Event Severity: Major
Event received: 28-Apr-2004, 17:03:47

Event description: Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.
User Action: Replace the storage system side panel.

Status: sidePanelRemoved

Example of Pager/SMS Page

From: Doe, John
Sent: Wednesday, April 28, 2004 5:04 PM
To: Doe, Jane
Cc: Smith, Jim; Jones, Beth
Subject: System A: Storage System side panel is removed
(Ver. 3): Pager
SMS Format E-mail testing

System A, Storage System side panel is removed (Ver. 3),Status:
sidePanelRemoved

Example of HTML Page

From: Doe, John
Sent: Wednesday, April 28, 2004 5:04 PM
To: Doe, Jane
Cc: Smith, Jim; Jones, Beth
Subject: qaunit1: Storage System side panel is removed (Ver. 3): HTML

Format E-mail testing

Event Identification and Details	
Event Severity	Major
Cleared Status	Not cleared
Event Source	quanit1
Associated System	quanit1
Associated System Status	Minor
Event Time	20-Apr-2004, 17:03:47 CDT
Description	Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel. User Action: Replace the storage system side panel.
Assignee	May-HTML
Comments	

Trap Details	
Variable Description	Value
An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.	GAUNTI
The Trap Flags. This is a collection of flags used during trap delivery. Each bit has the following meaning: Bit 5-31: RESERVED; Always 0. Bit 2-4: Trap Condition 0= Not used (for backward compatibility) 1= Condition unknown or N/A 2= Condition ok 3= Condition degraded 4= Condition failed 5-7= reserved Bit 1: Client IP address type 0= static entry 1= DHCP entry Bit 0: Agent Type 0= Server 1= Client NOTE: bit 31 is the most significant bit, bit 0 is the least significant.	0
Drive Box Side Panel Status. This value will be one of the following: other(1) The agent does not recognize the status. You may need to upgrade your software. sidePanelInPlace(2) The side panel is properly installed on the storage system. sidePanelRemoved(3) The side panel is not properly installed on the storage system. noSidePanelStatus(4) This unit does not support side panel status monitoring.	sidePanelRemoved

Where *quanit1* is the system name.

Related Procedures

- Managing Event Handling Tasks
- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Configuring Event Filters
- Configuring Modem Settings
- Configuring E-mail Settings

Related Topics

- Events
- About Administering Events

Service Notification Events

The HP Services analysis tools, Web-Based Enterprise Services (WEBES), and Open Service Event Manager (OSEM), generate service notifications to HP Systems Insight Manager (HP SIM) through a specific SNMP trap type if analysis has determined there are serviceable events.

This capability is supported in WEBES v4.4.1 or greater and OSEM v1.3 or greater, and has been part of HP SIM because version 4.0.

To download these tools and for installation instructions, go to:
<http://h18023.www1.hp.com/support/svctools/>.

OSEM can also be obtained from the *Smart Start Management CD* beginning with version 7.2.

If Instant Support Enterprise Edition (ISEE) is installed, the service notification provided by WEBES and OSEM also provide status about the remote support incident.

To download ISEE and for additional information, go to <http://h20219.www2.hp.com/services/cache/10709-0-0-225-121.aspx>.

Configuration and Setup

No special setup is required in HP SIM for the service notification to function properly because the Service Management Information Base (MIB) is part of the HP SIM kit and is compiled as part of the normal installation.

No special setup of WEBES or OSEM is required as long as these tools are on the same system as HP SIM because the service traps are normally sent to *localhost* by default. If WEBES or OSEM are on a separate system from HP SIM, then you must perform the procedure outlined in the *OSEM Installation Guide*, section *How to Change the HP SIM Host Name*.

In the case of WEBES, enter `desta snmp` from the operating system command line.

You are prompted for the system to send the service traps to and must enter the HP SIM system name regardless of whether WEBES and HP SIM are on the same system.

HP SIM Handling of Service Trap Notifications

Upon receipt of service trap notifications from WEBES or OSEM, HP SIM handles them in much the same way as any other management events.

There are several ways to view these events. One way is to view them under **All Events** as this is always done by default. Another way is to view them under event collections using the **Advanced Search** capability. For HP SIM 4.x, you must use Advanced Search and complete the following: Search for events where event category name is **HP Service Events** and type name is **any**. In HP SIM 5.0, this is done by default with the **All HP Service Events** located under **Events->Shared->All HP Service Events** in the **Systems and Events** panel panel.

On the event table view page, the **Event Type** is shown as **A Service Incident has been reported**. The **System Name** and **Event Time** refer to the failing system or subsystem and time the error was reported. The **Severity** is shown as Major because the service notification is only sent if analysis has determined that a maintenance action should be performed and because the service trap contains information in addition to what can be found in the original events such as SNMP traps sent by Insight Management Agents.

Service Trap Notification Details

To view details about the service notification from the event table view page, select the **A Service Incident has been reported** you are interested in under **Event Type** in the table to view the service trap itself.

The service trap consists of several types of information:

- Basic trap information, such as event identification, status, and description
- Source information identifying the attributes of the failing system and time of error
- URL link to WEBES or OSEM event analysis, which opens the WEBES or OSEM Event Viewer, providing detailed analysis and troubleshooting information specific to the event

- URL link to ISEE Client and provides call status for the particular event

Note:



This link is only available if ISEE is installed and status has been received properly from the ISEE client.

- Recommended action that provides information on the service action to perform to correct the problem and might include information such as failing location, system identification, and parts callout

Note:



This is only available in the Service MIB that ships with HP SIM 5.0 or greater and for service traps sent by OSEM 1.3.6 or WEBES 4.4.1.

- URL link to customer self-repair procedure, if available, and provides written instructions and videos to help you perform the recommended action.

Note: This is only available in the Service MIB that ships with HP SIM 5.0 or greater and for service traps sent by OSEM 1.3.6 or WEBES 4.4.1.

Service Trap and MIB Type Information

HP SIM 5.0 ships with a newer version of the Service MIB to support enhanced service traps sent by OSEM 1.3.6 and WEBES 4.4.1. OSEM 1.3.6 must be configured to generate the new trap type by going to Internal settings for OSEM: HP SIM trap revision. WEBES 4.4.1 sends the new trap by default.

The new MIB can be compiled into older versions of HP SIM 4.x and will recognize both the old and new versions of service traps. To obtain the latest service MIB, go to: <http://h18023.www1.hp.com/support/svctools/> and select **download service MIB** located under **WEBES** or **OSEM**. To register the new service MIB with HP SIM, perform the following procedure on the system running HP SIM.

1. Open an MS-DOS window or UNIX shell.
2. Change to the directory containing the MIBs.

- **For Windows:**

```
c:\program files\hp\systems insight manager\libs
```

- **For Linux:**

```
/opt/mx/mibs
```

3. Run `mxmib -d cpqservice.mib` to unregister the old service MIB.
4. Delete the old `cpqservice.mib` and `cpqservice.cfg`.
5. Copy the new `cpqservice.mib` to the `mibs` directory.
6. Run `mcompile cpqservice.mib` to compile the new service MIB into the `.cfg` format.
7. Run `mxmib -a cpqservice.cfg` to register the new service MIB.

Related Procedures

- Registering a MIB
- Unregistering a MIB

Related Topic

- Default Public Collections

Examples of Event Tasks

Examples for different event tasks that you might want to include in your portfolio include:

- **Deleting Cleared Server Events.** This example demonstrates how to create an event collection and creating and scheduling a task to delete cleared server events.
- **Deleting Information Events.** This example demonstrates how to create an event collection and creating and scheduling a task to delete informational events on a set schedule.
- **Send E-mail When a System Reaches a Critical State.** This example demonstrates how to create an event collection and creating and scheduling an Automatic Event Handling task to send an e-mail when systems reach a Critical state.
- **Creating a Paging Task.** This example demonstrates how to create an Automatic Event Handling task to send a page when a system reaches a Critical, Major, or Minor status.

Related Procedures

- Creating a Task to Delete All Cleared Events
- Creating a Task to Delete Events Older than Thirty Days
- Creating a Paging Task Based on E-mail Notification
- Creating a Task to Send an E-mail When a System Reaches a Critical State

Creating a Paging Task Based on E-mail Notification

You can set up a notification task that causes HP Systems Insight Manager (HP SIM) to send an e-mail that can then be forwarded to a BlackBerry, cell phone (for example, SMS), and other paging interface application whenever the central management server (CMS) receives a Critical, Major, or Minor event.

Important:



When using time filters, you can use on-call style e-mails or pages. If you want one person to be notified during business hours and another at night, create two different tasks and set the time filter appropriately.

Note:



This same type of task configuration can be applied to a Paging Task to use a modem in the HP SIM server to page through a BlackBerry or alphanumeric pager.

Note:



Paging is only supported on a CMS running Windows.

To create the task:

1. Select **Options->Events->Automatic Event Handling->New Task**. The **Automatic Event Handling - New Task** page appears.
2. Select **with event and system attributes that I will specify now** or **with an existing event collection**. Follow the steps to create the task.
3. In the **Task name** field, enter a name for the task, such as **Important Events for e-mail-Pager Task**.
4. Click **Next**. The **Select events** section appears. Refer to "Performing an Advanced Search for Events" for more information on selecting event criteria.
5. If a new event collection is to be created, then in the first selection box (criteria selection), select **severity**. Otherwise, a list of all event collections is displayed.
6. In the second selection box (comparison selection), select **is**.
7. In the third selection box (value selection), select **Critical**.
8. Click **Add** to add the Major and Minor severities to the task.
9. Repeat steps 5 through 6, and in the third selection box, select **Major** and **Minor**.
10. Click **Next**. The **Select systems** section appears. For more information on selecting system criteria, refer to "Performing an Advanced Search for Systems".
11. In the first selection box (criteria selection), select **system name**.

12. In the second selection box (comparison selection), select **is**.
13. In the third selection box (value selection), select **(any)**.
14. Click **Next**. The Select actions section appears.
15. Select **Send e-mail**.
16. In the **To** address field, enter the e-mail address to which you want the notification sent (multiple addresses can be added so that a group is notified). A **CC** address can also be added so that a manager or supervisor is also notified.
17. In the **Subject** field, enter your subject, for example, **HP Systems Insight Manager Events**.
18. In the **Message Format** section, change the option to **Pager/SMS**. This option sends a condensed e-mail format that is similar to a Paging Task in HP SIM, which is the ideal way to send alerts to a BlackBerry or cellphone type of hardware (or when TAPI is not available and an e-mail-to-paging provider is being used).
19. Click **Next**. The **Select time filter** section appears.
20. Select **Use time filter** and select **Nights and Weekends**, unless you want to receive the e-mail 24 hours per day. If so, clear **Use time filter**. Refer to "Applying a Time Filter" for more information on time filters.
21. Click **Next**. The **Review summary** appears.
22. Click **Previous** if you must make changes, or click **Finish** to save the task.

Related Procedures

- Creating an Automatic Event Handling Task with Selected Event and System Attributes
- Creating an Automatic Event Handling Task with an Existing Event Collection
- Managing Event Handling Tasks
- Scheduling a Task
- Applying a Time Filter

Creating a Task to Delete All Cleared Events

The following example describes how to create a task to delete all cleared server events from the HP Systems Insight Manager (HP SIM) database. This is a useful task to include in your management portfolio because deleting cleared events on a regular basis empties the database of unnecessary entries and improves system performance.

The following task has two segments:

- Creating an event collection that contains the events you want to delete
- Creating and schedule the task to delete all cleared server events and run the task

Creating the Event Collection

1. Select **Search** panel, click **Advanced Search**. The **Advanced Search** page appears.

2. Select **events** from the **Search for** dropdown list.
3. From the first selection box (criteria selection), click the down arrow, and select **cleared state**.
4. From the second selection box (comparison selection), click the down arrow, and select **is**.
5. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **cleared**.
6. Click **Add** to add the system type criteria.
7. From the first selection box (criteria selection), click the down arrow, and select **system type**.
8. From the second selection box (comparison selection), click the down arrow, and select **is**.
9. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **server**.
10. (Optional) Click **View** to view the search results.
11. Click **Save As** to save the event collection.
12. In the **Name** field, enter a name for the collection, such as **Delete Cleared Server Events**.
13. Under **Place in Folder**, select to save the collection in **Events by Severity** to have it available to other users.
14. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.

Creating and Scheduling the Task

1. Select **Options->Events->Clear Events**. The **Clear Events** page appears.
2. Select the **Delete Cleared Server Events** collection. Select **Select "Delete Cleared Server Events" itself**.
3. Click **Apply**.
4. Click **Schedule**.
5. In the **Task name** box, give the task a name, such as **Delete Cleared Server Events**.
6. In the **Refine schedule** section, select the scheduling option that you prefer. Refer to "Scheduling a Task" for more information on scheduling the task.
7. Click **Done**. The task is now scheduled and the **All Scheduled Tasks** page appears.

To run this task at any time, select **Tasks & Logs->View Task Results**. Then select **Delete Informational Events** from the table and click **Run Now**. Refer to "Running a Scheduled Task" for more information.

Related Procedures

- Performing an Advanced Search for Events
- Saving Collections

- Deleting Events from the Database

Related Topic

- Navigating the Tree View

Creating a Task to Delete Events Older than Thirty Days

Use this task to delete events based on a set of criteria. For example, you might create a task called Delete Informational Events, that deletes all informational events that are more than six weeks old.

Note:



You must have full-configuration-rights to delete security events.

Creating the Collection

1. Select **Search** panel, click **Advanced Search**. The **Advanced Search** page is displayed.
2. Select **events** from the **Search for** dropdown list.
3. From the first selection box (criteria selection), click the down arrow, and select **severity**.
4. From the second selection box (comparison selection), click the down arrow, and select **is**.
5. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **Informational**.
6. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **Normal**.
7. Click **Add** to select Normal severity.
8. From the first selection box (criteria selection), click the down arrow, and select **severity**.
9. From the second selection box (comparison selection), click the down arrow, and select **is**.
10. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **Normal**.
11. Click **Add** to select Normal severity.
12. From the first selection box (criteria selection), click the down arrow, and select **event time**.
13. From the second selection box (comparison selection), click the down arrow, and select **older than** and select **30 days**.
14. (Optional) Click **View** to view the search results.

15. Click **Save As** to save the event collection.
16. In the **Name** field, enter a name for the collection, such as **Delete Insignificant Events**.
17. Under **Place in Folder**, select to save the collection in **Events by Severity** to have it available to other users.
18. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.

Scheduling the Task

1. Select **Options->Events->Delete Events**. The **Delete Events** page appears.
2. Select the **Delete Insignificant Events** collection. Check the **Select "Delete Informational Events" itself** checkbox.
3. Click **Apply**.
4. Click **Schedule**.
5. In the **Task name** box, give the task a name, such as **Delete Informational Events**.
6. In the **Refine schedule** section, select **Every 1 week(s) on Saturday at 12:00 AM**, or select the day and time that you want the task to run.
7. Click **Done**. The task is now scheduled and the **All Scheduled Tasks** page appears.

To run this task at any time, select **Tasks & Logs->View Task Results**. Then select **Delete Informational Events** from the table and click **Run Now**. Refer to "Running a Scheduled Task" for more information.

Related Procedures

- Performing an Advanced Search for Events
- Creating a Task
- Scheduling a Task
- Deleting Events
- Saving Collections
- Running a Scheduled Task

Related Topic

- Navigating the Tree View

Creating a Task to Send an E-mail When a System Reaches a Critical State

The following instructions set up an automatic event handling task to be run when a discovered system goes to a Critical status.

Note:



There is a selection limit of 100 servers for automatic event handling tasks.

Creating the Collection

1. Select **Search** panel, click **Advanced Search**. The **Advanced Search** page is displayed.
2. Select **events** from the **Search for** dropdown list.
3. From the first selection box (criteria selection), click the down arrow, and select **severity**.
4. From the second selection box (comparison selection), click the down arrow, and select **is**.
5. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **Critical**.
6. (Optional) Click **View** to view the search results.
7. Click **Save As** to save the event collection.
8. In the **Name** field, enter a name for the collection, such as **Critical Events**.
9. Under **Place in Folder**, select to save the collection in **Events by Severity** to have it available to other users.
10. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.

Configuring HP SIM to Send E-mail

1. Select **Options->Events->Automatic Event Handling->E-mail Settings**. The **E-mail Settings** page appears.
2. Specify the SMTP host in the **SMTP Host** box.
3. Specify the e-mail address that the management server uses when sending e-mail notifications in the **Sender's Email Address** box.
4. To authenticate your SMTP server, select the **Server Requires Authentication** checkbox.
5. Specify the account name in **Account name** box.
6. Specify the password in the **Password** box.
7. Click **OK** to save changes.

Configuring Status Change Events

1. Select **Options->Events->Status Change Event Settings**. The **Status Change Event Settings** page appears.

2. Select **Enable creation of system status change events**. This option causes a system unreachable event to be sent whenever a system cannot be reached by a ping through the Hardware Status Polling task. Enabling this option causes a system reachable event to be created whenever the system is reachable again.
3. Click **OK** to apply changes.

Creating the Task

1. Select **Options->Events->Automatic Event Handling->New Task**. The **Automatic Event Handling - New Task** page appears.
2. Select **with an existing event collection**. There are five steps to define a the new task.
3. After selecting the option to use an existing event collection, there are five steps to define a new task. Step 1 **Select name**, is highlighted. Enter a name for the task in the **Task name** box, such as **Send E-mail for Critical Status**.
4. Click **Next**. Step 2, **Select existing event collection** page appears.
5. Select the **Critical Events** collection from the dropdown list.
6. Select **Send e-mail**.

- In the **To** field, enter the list of e-mail addresses that should receive the notification.

In the **CC** field, enter any e-mail address that should receive a copy of the e-mail, separating each with a comma.

In the **Subject** field, enter a note describing the subject of the e-mail.

In the **Message Format** field, select from the following formats based on the encoding preference of the recipient:

- Standard**. A default message format that sends a text e-mail message to the recipients
- Pager/SMS**. An e-mail message formatted with the same information and format as a pager message is sent to the recipients
- HTML**. An e-mail message that looks like the **HTML Event Details** page is sent to the recipients

In the **Encoding** field, select from the following formats:

- Western European (ISO-8859-1)**
- Unicode (UTF-8)**
- Japanese (ISO-2022-JP)**
- Japanese (Shift_JIS)**
- Japanese (EUC-JP)**

7. After you have made your selections, click **Next**.

- Step 4, **Select time filter** appears. Check the **Use time filter** box if you want to use time filters, and select an option from the dropdown list.

Click **Manage Filters** if you want to set user defined filters. Refer to “Applying a Time Filter” for more information.

- When you have entered the information, click **Next**.
- After clicking **Next**, Step 5, **Review summary** page appears. The **Task name**, the **selected event collection**, the **events**, **system criteria**, and **Action(s)** information are displayed. If you need to edit the e-mail selections, click **Edit e-mail Settings** to edit the SMTP settings. Refer to “Configuring SNMP Traps” for more information.
- Click **Finish** to create the new task.

Related Procedures

- Managing Event Handling Tasks
- Configuring E-mail Settings
- Configuring Event Filters

Status Polling

Polling Tasks track system health status for systems in the system list. It provides a simple means of assessing system health in the event that an SNMP trap or other event was not properly delivered to the Management console. Hardware status polling must occur continuously to determine when systems go offline or performance degrades. You can customize polling tasks for specific systems to run at scheduled times. You can also create new polling tasks with different system or event lists to match your specific requirements.

Note:



DMI Status polling is supported only on Windows central management servers and target systems.

There are two default Polling Tasks:

- **Software Status Polling.** Use Software Status Polling to determine software version update status. This task is set to run every seven days, on Wednesday at midnight, by default. You can edit the task and run it at any time. This task:

- Retrieves software and firmware inventory from systems
- Determines the software and firmware update status
- Sorts versions in the database

To access Software Status Polling, select **Options->Status Polling->Software Status Polling**.

- **Hardware Status Polling.** Used to track system status. There are two types of Hardware Status Polling Tasks:

- **Hardware Status Polling for Non-Servers.** Used to collect status information for target systems that are not of a server, cluster, or management processor type. This task is configured to poll every 10 minutes and at startup by default and does not send status change events.
- **Hardware Status Polling for Servers .** Used to collect status information for SNMP systems of type server, cluster, or management processor. This task is configured to poll every 5 minutes and at startup by default and sends status change events where you can set up a notification task based on the event.

To access Hardware Status Polling, select **Options->Status Polling->Hardware Status Polling.**

Related Procedures

- Hardware Status Polling
- Software Status Polling

Related Topic

- About Default Polling Tasks

Software Status Polling

The following example describes how to set up a Software Version Status Polling Task that determines whether managed systems have software that is out of date. This task uses the All Servers list as the default list.

Note:



One instance of this task is created by default when HP Systems Insight Manager (HP SIM) is installed. It runs on a weekly basis. Create this task only if it has been deleted.

To create a Software Status Polling Task:

1. Select **Options->Status Polling->Software Status Polling.**
2. Select target systems from the All Systems collection. The default selected is All Systems. Refer to “Creating a Task” for more information.
3. Click **Schedule** to schedule the task, or click **Run Now** to run the task immediately. Refer to “Scheduling a Task” for more information on scheduling the task.

Related Procedure

- Hardware Status Polling

Related Topics

- Status Polling
- About Default Polling Tasks

Hardware Status Polling

HP Systems Insight Manager (HP SIM) tracks system health status, using a predefined hardware status polling task. This task polls for updates on hardware status through the different protocols. The following example describes how to set up a task to poll systems using hardware status polling.

Note:



One instance of this task is created by default when HP SIM is installed. It runs when new systems or events meet the search criteria. Create this task only if it has been deleted.

To create a Hardware Status Polling Task:

1. Select **Options->Status Polling->Hardware Status Polling**.
2. Select the target systems. Refer to "Creating a Task" for more information.
3. Click **Next**. The **Select Protocol Settings** section appears.
4. Select from the following protocols:
 - DMI

Note: DMI is only available on Windows systems.

 - HTTP
 - SNMP
 - WBEM

Note: By default, all protocols are selected. If all protocols are unselected, then the **Schedule** and **Run Now** buttons are disabled.
5. Select **Timeout (in seconds)**:
 - **Use default (currently "4")**
 - **Use custom.** Timeout maximum is 120 seconds, with a minimum of 1 second.
6. Select the retry value:
 - **Use default (currently "1")**
 - **Use custom.** The retries maximum is 10 retries, with a minimum of 0 retries.
7. Select one of the following options to execute the task:
 - **Schedule.** Click **Schedule** to schedule when the task should run. Refer to "Scheduling a Task".

- **Run Now.** Click **Run Now** to run the task now. The **Task Results Page** appears. Refer to “Task Results List”.
- **Previous.** Click **Previous** to return to the previous page.

Related Procedure

- Software Status Polling

Related Topics

- Status Polling
- About Default Polling Tasks

WMI Mapper Proxy

The WMI Mapper proxy is a configuration setting for WMI. The WMI Mapper receives client CIM/XML WBEM requests and converts the requests to Windows Management Instrumentation (WMI) requests. The WMI results are converted to CIM/XML format and returned to the client. The discovery and Identification task uses the proxies in the WMI Mapper proxy list to discover whether a system is a WMI-enabled system. If the system is WMI-enabled, then the identification information for that system based on that specific proxy is returned.

The WMI Mapper proxy feature enables you to:

- **Add a WMI Mapper Proxy.** Select **Options>Protocol Settings>WMI Mapper Proxy>[New]**. The **Add WMI Mapper Proxy** section appears.
- **Edit a WMI Mapper Proxy.** Select **Options>Protocol Settings>WMI Mapper Proxy**. Select the proxy to edit and click **[Edit]**. The **Edit WMI Mapper proxy** section appears.
- **Delete a WMI Mapper Proxy.** Select **Options>Protocol Settings>WMI Mapper Proxy**. Select the systems to delete and click **Delete**. A confirmation box appears. Click **OK** to delete the systems or click **Cancel**, to cancel the deletion.

Note:



Sort any column by clicking the column heading.

Related Procedures

- Adding a WMI Mapper Proxy
- Editing a WMI Mapper Proxy
- Deleting a WMI Mapper Proxy

Related Topic

- Protocols

Adding a WMI Mapper Proxy

HP Systems Insight Manager (HP SIM) enables you to add a WMI Mapper proxy to define a new proxy for HP SIM.

Note:



You must have full-configuration-rights to add, edit, or delete a Windows Management Instrumentation (WMI) Mapper proxy.

To add a WMI Mapper proxy:

1. Select **Options->Protocol Settings->WMI Mapper Proxy->[New]**. The **Add WMI Mapper Proxy** section appears.
2. In the **Host** field, enter the full DNS name or IP address of the WMI Mapper proxy.
3. In the **Port number** field, enter a port number. The WMI Mapper proxy uses this port number to communicate with the WMI client.
4. Click **OK** to save and close the **Add WMI Mapper proxy** section. Click **Apply** to save without closing the **Add WMI Mapper proxy** section. Click **Cancel** to abort the save operation.

Related Procedures

- Editing a WMI Mapper Proxy
- Deleting a WMI Mapper Proxy

Related Topic

- WMI Mapper Proxy

Editing a WMI Mapper Proxy

Edit a Windows Management Instrumentation (WMI) Mapper proxy to update the proxy information. You can only edit one proxy at a time.

Note:



You must have full-configuration-rights to add, modify, or delete the WMI Mapper proxy.

To edit a WMI Mapper proxy:

1. Select **Options->Protocol Settings->WMI Mapper Proxy**.
2. Select the proxy to edit and click **Edit**. The **Edit WMI Mapper Proxy** section appears.
3. In the **Port number** field, change the port number. The WMI Mapper proxy uses this port number to communicate with the WMI client.
4. Click **OK** to save, or click **Cancel** to abort the edit operation.

Related Procedures

- Adding a WMI Mapper Proxy
- Deleting a WMI Mapper Proxy

Related Topic

- WMI Mapper Proxy

Deleting a WMI Mapper Proxy

HP Systems Insight Manager (HP SIM) enables you to delete a Windows Management Instrumentation (WMI) Mapper proxy. The delete option enables you to delete all selected proxies. Delete is available only if one or more proxies are selected.

Caution:



If you delete one or more WMI Mapper proxies, the deletion is permanent and the proxies cannot be restored.

Note:



You must have full-configuration-rights to add, modify, or delete the WMI Mapper proxy.

To delete a WMI Mapper proxy:

1. Select **Options->Protocol Settings->WMI Mapper Proxy**.
2. Select the systems you want to delete.
Note: Sort by any column by clicking that column heading.
3. Click **Delete**.

A message appears, asking you to confirm your intention to delete the WMI Mapper proxy.

4. Click **OK** to confirm your intention to delete the WMI Mapper proxy. Click **Cancel** to cancel the delete operation.

Related Procedures

- Adding a WMI Mapper Proxy
- Editing a WMI Mapper Proxy

Related Topic

- WMI Mapper Proxy

Protocols

Set protocol settings on a global basis that affect all systems, or set protocol settings for an individual system or group of systems.

To set protocol settings on a global basis access, the **Global Protocol Settings** page in any one of the following ways:

- Select **Options->Protocol Settings->Global Protocol Settings**.
- From the HP Systems Insight Manager (HP SIM) introductory page, click **Protocol Settings** in the **DO THIS NOW to finish the install** section.
- From the **Automatic Discovery - General Settings** page, click **Configure global protocol settings** in the **Discovery configuration** section.

To set protocol settings for a single system or group of systems, access the **System Protocol Settings** page in the following ways:

- From the **All Systems** page, click the **System Name** hotlink of the desired system to go to the **System Page** of that system, then click the **System Protocol Settings** hotlink on the **Tools & Links** tab page.
- Select **Options->Protocol Settings->System Protocol Settings**. Select the single system to set its protocol settings.

To set protocol settings for a single system, access the **System Protocol Settings** page by selecting **Tools->System Information->System Page**, and select a target system. Click **Run Now** and select **Links->System Protocol Settings**.

Related Procedures

- Setting Global Protocols
- Setting Protocols for a System or Groups of Systems
- Setting Protocols for a Single System

Related Topics

- Global Protocols

Setting Global Protocols

Set global protocols to configure default, system-wide protocol settings. These defaults apply to all newly discovered systems. For the passwords or community strings, the default list is iterated over until one of the strings works (if at all). HP recommends putting the most often used passwords or community strings first in the list.

Note:



In the following procedure, all sections are optional but highly recommended for proper management of systems.

Note:



If the **Global Protocol Settings** page is accessed from the **Automatic Discovery - General Settings** page, click **Automatic Discovery** at the top of the page to return to the **Automatic Discovery - General Settings** page. Otherwise, this option is not available.

To set global management protocol settings:

1. Select **Options->Protocol Settings->Global Protocol Settings**. The **Global Protocol Settings** page appears.
2. In the **Default ping settings** section, select **Use the ICMP protocol for system reachability (ping) check** or **Use the TCP protocol for system reachability (ping) check port number 80**. The **Use the ICMP protocol for system reachability (ping) check** is the default and recommended setting.

Select **Use the TCP protocol for system reachable (ping) check. port number 80** if your company has disabled ICMP on the corporate network or the corporate policy mandates system firewall software to filter out ICMP requests. For example, Windows XP has this feature built in and can result in systems not being automatically discovered. This option enables you to run HP Systems Insight Manager (HP SIM) and ping all available systems.

Note: This option only applies to IP-based systems and is available for global, system-wide settings that are used when managing all systems in HP SIM. It is used by automatic discovery, hardware status polling, the ping tool, and any other tool that must verify system availability. This option is not available on a single-system basis.

Note: If you select **Use the TCP protocol for system reachable (ping) check. port number 80**, even though HP SIM attempts a connection request to the current system, that system does not need any additional software running on it for this option to work. For example, HP does not require that a Web server be running on port 80. Some networking systems might not respond to the TCP request, which is typically seen in low end networking equipment. Manual additions can be made if it is necessary. However, this system displays as Critical if hardware status polling is run.

3. Also in the **Default ping settings** section, set the **Default timeout** and the **Default retries**. If some systems are managed over a WAN or satellite link, use a larger timeout (for example, 5 seconds) with at least one retry. For a LAN, a shorter time-out can be used. This can be configured on a single-system basis. Refer to “Setting Protocols for a System or Groups of Systems” for more information on setting single-system protocols.
4. In the **Default WBEM settings** section, select **Enable WBEM** to allow Web-Based Enterprise Management (WBEM) requests to be sent. Enabled is the default setting. Enter as many default user names and passwords as needed. If your network includes storage systems, enter the user name and password of each SMI CIMOM in this section. The identification process attempts each of these user name and password pairs until a successful response is obtained. Future WBEM requests to that system use the user name and password that succeeded. For Windows-based systems, the user name should include the domain name, for example, *domainname\username*.

Note: Order the name and password pairs such that root and administrator passwords are listed first and user and guest passwords are listed second. This order minimizes the search time.
5. In the **Default HTTP settings** section, select **Enable HTTP and HTTPS** if it is necessary to allow Web-based agents and other HTTP port scans to be identified. HP recommends leaving this option enabled for proper management and discovery of systems.
6. In the **Default SNMP settings** section, select **Enable SNMP**, which is the system default, and set the **Default timeout** and **Default retries**. If some systems are managed over a WAN or satellite link, use a larger timeout (for example, 5 seconds) with at least one retry. For a LAN, a shorter timeout can be used. These settings can also be configured on a single-system basis.
7. Enter the **Default write community string**. This value is case-sensitive. Only a few tools need this option set. Community strings are case-sensitive.
8. Enter the **Read community string**. This value is case-sensitive. Enter as many as needed. The identification process attempts communication to the system, using each of these communities in succession until a successful response is obtained. Future SNMP requests then use the community string that provided a successful response.
9. In the **Default DMI settings** section, select **Enable DMI**, which is the default setting, to enable Desktop Management Interface (DMI) identification to run on systems. DMI is used to manage some older desktops, HP-UX servers, and some third-party servers. If you do not need to manage these kinds of systems, DMI can be disabled to improve discovery performance.

Note: DMI is not currently supported on Linux systems and is not shown in the user interface.

Note: If DMI is disabled and some systems no longer have a correct system type or product name, re-enable DMI.

Note: DMI identification is only supported on Windows and HP-UX-based central management server (CMS) installs. In addition, only like operating systems can be identified. For example, Windows-based CMSs can identify Windows-based DMI, and HP-UX-based CMSs can only identify HP-UX-based DMI systems.
10. Click **OK** to accept the settings.

If you accessed this page from the **Discovery** page, click **automatic discovery** to return to the **Discovery** page after making changes.

Related Topics

- Protocols
- Global Protocols

Setting Protocols for a System or Groups of Systems

Configure single-system protocol settings to fine-tune settings for individual systems or a group of similar systems. This option is especially useful if some of your systems are accessed through a LAN while others are accessed through a WAN. Configure systems accessed through the WAN with longer timeouts and increased retries.

Note:



If you have chosen a collection when first using this tool, you can click the collection link at the top of the page. A pop-up window appears, showing all systems in the collection chosen. Click **OK** to close the window. This link is not displayed if you have chosen a single system.

To set protocol settings for a single system or a group of similar systems:

1. Select **Options->Protocol Settings->System Protocol Settings**.
2. Select the target systems. Refer to "Creating a Task" for more information.
3. Click **Next**.
4. In the **Ping (ICMP) settings** section, select **Update values for this protocol** to enable updating the ICMP settings. If this is not selected, the settings are not updated. This is disabled by default.
5. In the **Ping (ICMP) settings** section, select:
 - **Use global defaults.**
 - **Use values specified below.** Enter the **Timeout (seconds)** and the **Retries**.
6. In the **WBEM settings** section, select **Update values for this protocol** to enable updating the WBEM settings. If this is not selected, the settings are not updated. This is disabled by default.
7. In the **WBEM settings** section, select:
 - **Use global defaults.**
 - **Use values specified below.** Enter the **Port #**, **User name** (for Windows based systems, the user name should include the domain name, for example *domainname/username*), the **Password**, and **Confirm Password**.

Enter as many sets of these values as needed.

Note: The **Port #** can be blank for a set if appropriate.

8. In the **SNMP settings** section, select **Update values for this protocol** to enable updating the SNMP settings. If this is not selected, the settings are not updated. This is disabled by default.
9. In the **SNMP settings** section, select:
 - **Use global defaults.**
 - **Use values specified below.** Enter the **Timeout (seconds)**, **Retries**, **Read community string**, and the **Write community string**.
10. In the **SSH settings** section, select:
 - **Not applicable.**
 - **Use values specified below.** Enter the **User name**, **Password**, and **Confirm password**.

Note:



Information should be included in this section if your target Secure Shell (SSH) server does not support public key authentication.

11. In the **Identification settings** section, **Also run system identification** is selected by default. If you do not want to run system identification, deselect this box.
12. Click **Previous** to return to the previous screen without saving any changes, click **Schedule** to schedule the task, or click **Run Now** to run the task immediately. Refer to “Scheduling a Task” for more information on scheduling tasks.

Note: If the **Schedule** and **Run Now** buttons are disabled, look for bold red error messages and correct all of the problematic entries, to enable these buttons.

Related Procedures

- Setting Global Protocols
- Setting Protocols for a Single System

Related Topics

- Protocols
- Global Protocols

Setting Protocols for a Single System

Configure single-system protocol settings to fine-tune settings for an individual system.

To set protocol settings for a single system:

1. Select **Tools->System Information->System Page**.

2. Select target systems. Refer to “Creating a Task” for more information.
3. Click **Run Now**. The **System Page** appears.
4. Select the **Tools & Links** tab.
5. Under **HP SIM Pages**, click **System Protocol Settings**. The **System Protocol Settings** page appears.
6. In the **Ping (ICMP) settings** section, select **Update values for this protocol** to enable updating the ICMP settings. If this is not selected, the settings are not updated. This is disabled by default.
7. In the **Ping (ICMP) settings** section, select:
 - **Use global defaults.**
 - **Use values specified below.** Enter the **Timeout (seconds)** and the **Retries**.
8. In the **WBEM settings** section, select **Update values for this protocol** to enable updating the WBEM settings. If this is not selected, the settings are not updated. This is disabled by default.
9. In the **WBEM settings** section, select:
 - **Use global defaults.**
 - **Use values specified below.** Enter the **Port #**, **User name** (for Windows based systems, the user name should include the domain name, for example *domainname/username*), the **Password**, and **Confirm Password**.

Enter as many sets of these values as needed.

Note: The **Port #** can be blank for a set if appropriate.
10. In the **SNMP settings** section, select **Update values for this protocol** to enable updating the SNMP settings. If this is not selected, the settings are not updated. This is disabled by default.
11. In the **SNMP settings** section, select:
 - **Use global defaults.**
 - **Use values specified below.** Enter the **Timeout (seconds)**, **Retries**, **Read community string**, and the **Write community string**.
12. In the **SSH settings** section, select **Update values for this protocol** to enable updating the SSH settings. If this is not selected, the settings are not updated. This is disabled by default.
13. In the **SSH settings** section, select:
 - **Not applicable.**
 - **Use values specified below.** Enter the **User name**, **Password**, and **Confirm password**.

Note: Information should be included in this section if your target Secure Shell (SSH) server does not support public key authentication.

14. In the **Identification settings** section, **Also run system identification** is selected by default. If you do not want to run system identification, deselect this box.
15. Click **OK** to save the settings, or click **Return to System Page** to return to the **System Page** for the system and not save changes.

Note:



If the **OK** button is disabled, look for any bold red error messages and correct all the problematic entries to enable that button.

Related Procedures

- Setting Protocols for a System or Groups of Systems
- Setting Global Protocols

Related Topics

- Protocols
- Global Protocols

Global Protocols

Managing a network is complex, and network management becomes even more complicated without standards. When an organization purchases multiple management tools, each with a different method of managing a particular hardware or software product, it must maintain and train network administrators in different tools. This process is both expensive and inefficient. To address this issue, standards committees have developed protocols for network management.

HP Systems Insight Manager (HP SIM) takes advantage of many different management protocol standards. This capability enables HP SIM to provide management support for a wide array of manageable devices.

SNMP

The Internet Engineering Task Force (IETF), the standards-rating body for the worldwide Internet network, has defined a management protocol, SNMP, which has accumulated a major share of the market and has the support of over 20,000 different products. SNMP has its roots in the Internet community. The complexity of large international TCP/IP networks has provided the necessary incentive to develop a standard method of managing devices on the network.

Within the SNMP framework, manageable network devices (routers, bridges, servers, and so on) contain a software component called a management agent. The agent monitors the various subsystems of the network element and stores this information in a Management Information Base (MIB). The agents enable the device to generate traps, which can be configured to be sent to a trap destination server that is running HP SIM. Conceptually, the MIB is a database that can be

written to and read by a management application using the SNMP protocol. There are two types of MIBs:

- **Internet Management MIBs.** These MIBs, standardized by the Internet community, include MIB-II, RMON, and others and represent the core objects that are common across the widest range of network devices implementing the Internet protocols. Examples of these objects include network protocols such as TCP/IP and network systems such as Ethernet network interfaces.
- **Vendor MIBs.** These MIBs represent objects that are unique to an individual vendor's product or product line. Over 500 vendors and organizations have created their own vendor MIBs. HP was the first personal computer company to develop a MIB-enabled SNMP management of system hardware.

SNMP supports both read and write (**GET** and **SET**) commands on attributes. Some vendors do not support the **SET** command because of the potential to allow an unauthorized person to alter critical parameters on a network element. HP SIM primarily only uses the SNMP **GET** command.

SNMP is associated with TCP/IP and used for monitoring devices on Ethernet networks because of its long association with the Internet. However, you can use SNMP over other protocols such as IPX. For example, the HP SIM application supports SNMP over IPX and IP.

Since its inception, SNMP itself has undergone several updates, including SNMP V2c and SNMP V3. HP SIM supports the original V1-compliant agents and the compilation of V1 and V2 MIBs. SNMP uses UDP port 161 for monitoring systems while traps are received on port 162.

SNMP communication between systems is used to gather information about a system. HP SIM attempts SNMP communications based on the number of SNMP retries you specify and only stops when the communication is successful or the number of retries is exceeded. HP SIM also waits for SNMP responses between retries, based on the timeout period. Finally, HP SIM can only communicate through SNMP when the community string specified on the system and the community string specified for that system in HP SIM match. The community string, "public," is a commonly used default. However, you can specify any community string needed for your security requirements.

Note:



Community strings on the managed system and the HP SIM community strings for the system must match to manage the system through SNMP. Some SNMP management agents also provide IP address filtering. Be sure the HP SIM IP address is in the allow list for any given SNMP agents.

DMI

The Desktop Management Task Force (DMTF), formed in 1992 and composed of leading PC industry vendors and corporations, established a common, platform-independent process for specifying methods of managing desktop hardware and software components. HP is a Steering Committee member of the DMTF and helped to define the task force's two pieces of technology: the Desktop Management Interface (DMI) software and the Management Information Format (MIF) language. DMI software serves as the liaison between desktop-resident management programs, manageable hardware, and software components on the computer. DMI is most commonly used for obtaining information from desktops, but some HP servers and workstations do support DMI.

HTTP

HP SIM also takes advantage of the industry-standard HTTP protocol (used to transfer information over the World Wide Web) for transportation of management information. Many systems support some kind of configuration "home page" that is supported over HTTP or the secure HTTPS protocol. HP SIM attempts to find HTTPS servers running on systems if the **Global Protocol Settings** page has this enabled. Refer to "Setting Global Protocols" for more information.

WBEM

Web-Based Enterprise Management (WBEM) is one of the newest management protocols. This protocol leverages the industry-standard Common Information Model (CIM) as defined by the DMTF. HP SIM can communicate to systems directly using the WBEM protocol, or to the Windows WMI systems using the WMI Mapper Proxy. HP SIM uses WBEM to communicate with storage system SMI-S WBEM providers. HP has been leading this effort through its association with the WBEM initiative. WBEM is an initiative supported by HP, Microsoft, Intel, BMC, Cisco, and 120 other platform, operating system, and application software suppliers.

When WBEM is enabled, the management console can obtain information from any system that supports WBEM. For WBEM to work, the correct user name and password must be provided for the given system. WBEM enables a larger set of server and storage manageability data to be collected and displayed on the **System Page** and in reports. The presence of WBEM enables the **Properties** pages and enables WBEM indications (events) to be displayed in event collections. Without HTTP enabled, HP SIM will not discover any Web-based features on a system.

Note:



HP SIM supports WBEM over HTTPS to ensure user supplied WBEM name and password pairs are protected.

Related Procedures

- Setting Global Protocols
- Setting Protocols for a System or Groups of Systems

Related Topics

- Protocols
- WMI Mapper Proxy

Data Collection

Data collection is used to gather data that can be used for reporting. There are two ways that this data can be collected and stored in the database. You can choose to maintain only the most recent data, enabling you to run reports, or compare different systems to each other using Snapshot Comparison. Additionally, you can store all of the data collected over time, which enables you to use Snapshot Comparison to view trends on a single system

Data collection uses SNMP, Desktop Management Interface (DMI), Web-Based Enterprise Management (WBEM), or a combination of the three protocols to gather information, which ensures you a comprehensive dossier on a system. Typically, DMI is instrumented on Windows-based desktop computers and laptops and on HP-UX systems. SNMP is instrumented on Windows-based servers, Linux systems and other networking systems, and can be used to interrogate Windows-based desktops. The WBEM protocol is used to collect data from storage systems such as arrays, tape libraries, Fibre Channel switches, and HBAs. Data can be collected from any storage system with an SMI-S provider that complies with the Storage Networking Industry Association's Storage Management Initiative Specification. Refer to the HP Systems Insight Manager Installation and User Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information about SMI-S providers.

After HP Systems Insight Manager (HP SIM) collects data initially, you can schedule a Data Collection task to specify systems and run the task with different schedules. In addition to the default Initial and Bi-Weekly Data Collection tasks built into HP SIM, you can set up new data collection tasks targeting specific managed systems. If you are scheduling to **Overwrite existing data set (for detailed analysis)**, formerly known as Single Instance Data Collection task in Insight Manager 7, having it run once per week (smaller networks) to once per month (larger networks) should be adequate. If you are scheduling to **Append new data set (for historical trend analysis)**, formerly known as Historical Data Collection task in Insight Manager 7, it might be beneficial to run it more frequently, perhaps once per hour for your most important systems, realizing it consumes database storage space.

To create a Data Collection task from the toolbar, select **Options->Data Collection**.

Note:



The Data Collection Report does not display CPU information for Netware systems.

Note:



To enable data collection to collect data from any of the aforementioned instrumentation protocols, the corresponding protocol must be enabled, and the appropriate protocol settings must be specified, globally or for the specific target system. Refer to "Setting Global Protocols" for more information on setting global protocol settings and "Setting Protocols for a System or Groups of Systems" for more information on setting single system protocol settings.

Note:



To enable collection of DMI data from a DMI-instrumented HP-UX system, be sure that the name of the server that the HP SIM runs on is added to the `/var/dmi/dmimachines` file of the target system.

Note:



To enable collection of Windows Management Instrumentation (WMI) data from WMI-instrumented systems, a WMI Mapper Proxy must have been set up and specified through **Options->Protocol Settings->WMI Mapper Proxy**. Refer to “Adding a WMI Mapper Proxy” for information on setting up a WMI Mapper Proxy.

Append New Data Set (for Historical Trend Analysis)

The **Append new data set (for historical trend analysis)** option maintains trend information in separate historical entries. You can use the historical perspective for trend and usage analysis because records change over time. Information gathered by data collection is used in Snapshot Comparison and reports and can be used as criteria in system collections. With **Append new data set (for historical trend analysis)**, data detailing the system history is collected. Use **Append new data set (for historical trend analysis)** conservatively and sparingly to track problem systems or problem usage times. Do not overuse this task because it can create considerable amounts of data to be stored.

Caution:



Do not delete the standard data collection task without replacing it with a substitute task that achieves a similar result. For example, removing the Data Collection task removes the capability for historical analysis and updating any information shown in reporting tables. You must refresh the page to see new data in reports.

Overwrite Existing Data Set (for Detailed Analysis)

The **Overwrite existing data set (for detailed analysis)** option overwrites any previous information collected. The **Overwrite existing data set (for detailed analysis)** is useful as a snapshot at the current time because it overwrites old information with the current value.

You can view the current data set report from the **System Page**, which you can reach by selecting a system in a collection. Refer to “System Page” for information on the **System Page**.

Running data collection consumes noticeable network resources. Proper scheduling might be appropriate.

Important:



Multiple instances of the same Status Polling or Data Collection tasks do not run simultaneously.

Initial Data Collection

The Initial Data Collection task is used to collect information from many systems that have DMI, SNMP, or WBEM running, for example, serial numbers and model numbers. This task is set to run by default when a new system or event meets the search criteria. You can view the Data Collection Report for a system after data has been collected by selecting it from the system table view page. This action displays the **System Page**, where you can select the **Data Collection Report** link from the **Tools & Links** tab. Other report formats are available from the Reporting tool. Refer to “Reporting” for more information on reporting.

Bi-Weekly Data Collection

The Bi-Weekly Data Collection task runs the **Overwrite existing data set (for detailed analysis)** option on all of the systems in the system default collection. The default schedule is to run every two weeks on Saturday at 12:00 am. You can view the Data Collection Report for a system after data has been collected by selecting it from the system table view page. This action displays the **System Page**, where you can select the **Tools & Links** tab and then click **Data Collection**.

Related Procedure

- Creating a Data Collection Task

Related Topics

- Discovery and Identification
- Protocols
- Reference Information
- System Page
- Reporting

Creating a Data Collection Task

Data collection is used to gather data that can be used for reporting. There are two ways you can collect this data. You can collect detailed data to use for reporting, or for comparing different systems with Snapshot Comparisons, or you can collect less detailed data, but collect it over time. This enables you to use Snapshot Comparisons to view trends on a single system.

To create a Data Collection task:

1. Select **Options->Data Collection**. The **Data Collection** page appears.
2. Select target systems. Refer to “Creating a Task” for more information.
3. Click **Next**.
4. Specify how to save data by selecting:
 - **Overwrite existing data set (for detailed analysis)**. Provides a network snapshot at a certain time
 - **Append new data set (for historical trend analysis)**. Provides trend and usage analysis

5. Select one of the following options to execute the task:
 - Click **Schedule** to schedule when the task should run. Refer to “Scheduling a Task”.
 - Click **Run Now** to run the task now. The **Task Results Page** appears. Refer to “Task Results List”.
 - Click **Previous** to return to the previous page.
6. Click **Done**.

View the task results by selecting the desired data collection task on the **All Scheduled Tasks** page. Refer to “Task Results List” for more information on the All Scheduled Tasks page.

Command Line Interface

Use the `mxtask` command to perform this task from the command line interface. For assistance with this command, refer to the HP-UX or Linux manpage by entering `mxtask` at the command line or the Windows command help. Refer to “Using Command Line Interface Commands” for information on accessing the manpage.

Related Topics

- Data Collection
- Reference Information

System Properties

The Set System Properties tool enables you to set system properties for a single system or for multiple systems.

Note:



System properties that are edited in HP Systems Insight Manager (HP SIM) are not transferred to HP Storage Essentials.

There are two options for setting system properties:

- **Edit system properties for a single system.** Select the **Tools & Links** tab on the **System Page** and click the **Edit System Properties** link.
- **Set system properties for multiple systems.** Select **Options->System Properties->Set System Properties**.

The Suspend or Resume Monitoring tool enables you to suspend monitoring of a single system or multiple systems. This enables systems to be excluded from status polling, identification, data collection, and the automatic event handling features of HP SIM. The available suspend lengths include the predetermined increments of five minutes, 15 minutes, one hour and one day. The suspend tool can also be turned on indefinitely. Configuration changes take effect immediately. To view the new settings for a system, select the **Identity** on the **System Page**. Changes made

with this tool override previous settings. A system that is suspended appears with a disabled icon throughout HP SIM.

There are two ways to suspend or resume monitoring:

- **Suspend or resume monitoring for a single system.** Select the **Tools & Links** tab on the **System Page** and click the **Suspend/Resume Monitoring** link.
- **Suspend or resume monitoring for multiple systems.** Select **Options->System Properties->Suspend or Resume Monitoring**.

Note:



You must have full-configuration-rights to access these tools.

Related Procedures

- Editing System Properties for a Single System
- Editing System Properties for Multiple Systems
- Suspending or Resuming System Monitoring for a Single System
- Suspending or Resuming System Monitoring for Multiple Systems

Related Topics

- System Page

Editing System Properties for a Single System

The **Edit System Properties** link enables users with full-configuration-rights to re-configure system properties for a single system through its **System Page** which is made up of the following sections.

- **Identification.** This section includes the following information:
 - **Preferred System Name.** With this property, you have the capability to specify how the system (including the CMS) appears in the HP Systems Insight Manager (HP SIM) user interface. The **Restore Default Name** button sets the displayed name back to the name originally discovered by HP SIM.

Note:



If you change the preferred name, a warning message appears stating that any lists referring to this system by name might no longer work, and any subsequent discoveries of a system using the new name causes the system name change to be changed back to the host (DNS) name.

- **Prevent the Discovery process from changing this system name.** When checked, this prevents Discovery from overwriting the preferred system name.

- Serial number.** This is the serial number of the system. Any user-entered value will be overwritten by Identification, regardless of the checkbox setting described below. This field is read only if it is set by Discovery.

- **Product Description.** All properties are configurable.
 - System type.** This is the System type for the system, click the down arrow and select the appropriate System type.
 - System subtype 1 - 8.** This is the System subtype for the system, click the down arrow and select the appropriate System subtype. You can provide up to eight different system subtypes.
 - Product model.** This is a free form field and you can enter the system model number here.
 - Hardware description.** This is a free form field describing the hardware.
 - Operating system description.** This is the name of operating system running on the system, if any.
 - Operating system for tool filtering.** This is the operating system for tool filtering, click the down arrow and select the operating system (HP Unix, Linux, Novell, Tru64 Unix, or Windows).
 - Operating system version.** This is a free form field and is the operating system version.

- **Contact Information.**
 - Contact.** This is a free form field and is the contact user for the system.
 - Location.** This is a free form field and is the physical location of the system.

- **Asset Information.** This is the asset number of the system and is retrieved through the Data Collection process.
 - Asset number.** This is the asset number of the system and is retrieved through the Data Collection process.

- **Prevent the Discovery, Identification, and Data Collection processes from changing these system properties.** When checked, Discovery, Identification, and Data Collection do not overwrite any of the property values. However, when deselected, the Discovery, Identification, and Data Collection processes might overwrite or clear the properties. One exception to this behavior is with the serial number which is overwritten with any serial number obtained through Identification, regardless of this checkbox setting.

Note:



If this box is deselected and you click **OK**, HP SIM checks to see if any changes have been made. If so, a warning message appears stating that your changes might be overwritten by the next Discovery. To avoid having Discovery overwrite your changes, you should check this box.

To reconfigure system properties:

1. From the **System Page**, select the **Tools & Links** tab.

2. Click the **Edit Systems Properties** link to reconfigure the systems properties for an individual system. The **Edit System Properties** page appears.
3. Edit any desired fields.
Note: If the serial number field was set by discovery, you cannot edit it.
4. Click **OK** to apply the attribute changes or click **Cancel** to cancel all changes. After clicking **OK** or **Cancel**, you are returned to the **Tools & Links** tab.

Note:



Changing system properties might affect collection results. Changing the **Preferred System Name** of a system affects any system-by-name collections that the user has created. Changing the System type affects any by-system-type collections.

Refer to “Editing System Properties for Multiple Systems” for information on setting system properties for multiple systems.

Related Procedure

- Editing System Properties for Multiple Systems

Related Topics

- System Page
- Tools & Links Tab
- Editing System Properties for Multiple Systems

Editing System Properties for Multiple Systems

This tool enables you to edit system properties for multiple systems at one time. The **Set System Properties** page for multiple systems is similar to the **Edit System Properties** page for a single system, except that a checkbox appears next to each property. The checkboxes enable you to select the properties you want to configure when the tool executes. Only the checked properties are saved as a property for the target systems. If the value of the selected property is blank, that property is not set for the systems. All properties are optional.

Note:



This tool does not affect systems that are managed by HP Storage Essentials.

Note:



This tool can be used for a single system. However, some of the properties that are available from the **System Page** are not available when selecting this option. For example, the serial number is not available here, whereas, it is available from the **System Page**.

To edit system properties for multiple systems:

1. Select **Options>System Properties>Set System Properties**. The **Set System Properties** page appears.
2. Select target systems. Refer to “Creating a Task” for more information.
3. Click **Next**.
4. Under **Identification**, select **Restore the default system name** to change the name displayed in HP Systems Insight Manager (HP SIM) to the host (DNS) name.
5. Under **Product Description**, select the properties you want to configure. The properties include:
 - **System type.** This is the system type for the system, click the down arrow and select the appropriate System type.
 - **System subtype 1 - 8.** This is the system subtype for the system, click the down arrow and select the appropriate system subtype. You can provide up to eight different system subtypes.
 - **Product model.** This is a free form field and you can enter the system model number here.
 - **Hardware description.** This is a free form field describing the hardware.
 - **Operating system description.** This is the name of operating system running on the system, if any.
 - **Operating system for tool filtering.** This is the operating system for tool filtering, click the down arrow and select the operating system (HP Unix, Linux, Novell, Tru64 Unix, or Windows.)
 - **Operating system version.** This is a free form field and is the operating system version.
6. Under **Asset Information**, select the **Asset number** and enter the asset number of the system.
7. Under **Contact Information**, select from:
 - **Contact.** This is a free form field and is the contact user for the system.
 - **Location.** This is a free form field and is the physical location of the system.

8. Under **System Property Lock**, select from:
 - **Lock - Prevent the Discovery and Identification processes from changing any system properties.** The attribute lock setting of the target systems is set, preventing discovery and Identification from overwriting its properties.
 - **Unlock - Allow the Discovery and Identification processes to change system properties.** The attribute lock setting of the target systems are cleared, enabling discovery and Identification to overwrite its properties.
 - **Ignore - Do not set the lock property of the target systems.** The current attribute lock setting of the target systems remain unchanged.
9. Click **Previous** to select different target systems, click **Schedule** to schedule the task, or click **Run Now** to run the task immediately.

Refer to “Editing System Properties for a Single System” for information on setting system properties for a single system.

Related Procedure

- Editing System Properties for a Single System

Related Topics

- System Page
- Tools & Links Tab

Suspending or Resuming System Monitoring for a Single System

The **Suspend/Resume Monitoring** link enables you to set the timer for suspending monitoring. The Suspend or Resume Monitoring command has no effect on HP Storage Essentials systems.

Note:



You must have full-configuration-rights to access this feature.

To suspend or resume system monitoring on a single system:

1. Select **Tools->System Information->System Page**. The **System Page** appears.

Note: You can also access the **System Page** by selecting a system name in the **System Name** column of the system table view page.

2. Select the target system. Refer to “Creating a Task” for more information.
3. Select the **Tools & Links** tab.

4. Click the **Suspend/Resume Monitoring** link. The **Suspend/Resume Monitoring** page appears.
5. Select one of the following options:
 - **Enable monitoring of this system.** Select this option if you no longer want the system to be suspended.
 - **Suspend monitoring of this system for.** Select this option if you want to suspend a system for a set amount of time. Set the time by clicking the dropdown arrow and selecting an option.
 - **Suspend monitoring of this system indefinitely.** Select this option to suspend a system until it is set otherwise.
6. Click **OK** to apply the changes or click **Cancel** to cancel changes. After clicking **OK** or **Cancel** you are returned to the **Tools & Links** tab.

Refer to “Suspending or Resuming System Monitoring for Multiple Systems” for information on suspending or resuming monitoring for multiple systems.

Related Procedure

- Editing System Properties for Multiple Systems

Related Topics

- System Page
- Suspending or Resuming System Monitoring for Multiple Systems

Suspending or Resuming System Monitoring for Multiple Systems

The Suspend or Resume Monitoring tool enables you to set the timer for suspending monitoring of multiple systems. The Suspend or Resume Monitoring tool has no effect on HP Storage Essentials systems.

Note:



You must have full-configuration-rights to access this feature.

To suspend or resume system monitoring for multiple systems:

1. Select **Options->System Properties->Suspend or Resume Monitoring**. The **Suspend or Resume Monitoring** page appears.
2. Select target systems. Refer to “Creating a Task” for more information.

3. Click **Next**. You can click **Add Targets** to add additional systems or select targets and click **Remove Targets** to remove the systems.
4. Select one of the following options:
 - **Enable monitoring of target systems.** Select this option if you no longer want the target systems to be suspended.
 - **Suspend monitoring of target systems for.** Select this option if you want to suspend target systems for a set amount of time. Set the time by clicking the dropdown arrow and selecting an option.
 - **Suspend monitoring of target systems indefinitely.** Select this option to suspend target systems until it is set otherwise.
5. Click **Previous** to select different target systems, click **Schedule** to schedule the task, or click **Run Now** to run the task immediately.

Refer to “Suspending or Resuming System Monitoring for a Single System” for information on suspending or resuming monitoring for a single system.

Related Procedure

- Suspending or Resuming System Monitoring for a Single System

Related Topics

- System Page
- Identity Tab for Servers
- Tools & Links Tab

Version Control Repository

HP Systems Insight Manager (HP SIM) enables you to specify a HP Version Control Repository Manager. The VCRM stores the latest ProLiant Support Packs providing the latest software.

To specify a Version Control Repository,;

1. Select **Options->Version Control Repository**. The **Version Control Repository** page appears.
2. Under **Select the default version control repository**, select a system that has the VCRM installed.

Note: The system that has the VCRM installed must be trusted. Refer to “Trusted Certificates” for more information regarding trust relationships. After the trust relationship is established, click **Last Update** to update the **Trusted?** column to **Yes**.

3. Under **Contents of selected version control repository**, click the  icon to drill down and view the contents of the selected Version Control Repository

Note: To expand the tree to display all contents, click the  icon, located in the upper right corner of the **Contents of selected version control repository** section. Click the  icon to collapse the listings.

Note: Click any column heading to sort by that column in ascending or descending order.

Note: This section displays systems that are authorized by the current user. If the current user is not authorized to view any systems with the HP Version Control Repository Manager, the system will not be listed in the **Select the default Version Control Repository** section. If there are no discovered systems running the VCRM, a message appears, indicating that no repository could be found.

4. Click **OK** to apply your selection. A message appears, indicating if the repository setting was successfully saved.
5. Click **OK** to close the dialog box.

Related Topics

- Version Control
- About the Version Control Repository Manager
- About the Version Control Agent

PMP Administrative Options

Three Performance Management Pack (PMP) administrative tools are available through HP Systems Insight Manager (HP SIM):

- **Licensing.** Enables you to apply licenses to servers and add additional licenses to PMP.

To access **Licensing**, select **Options->Performance Management Pack Options->Licensing**.

To access help for this option, go to

https://middle_tier:2381/pmp/help/License_Administration.htm where *middle_tier* is the name or IP address of the server that HP SIM and PMP are installed, or access *PMP directory*\Program Files\HP\Performance Management Pack\PMP\htm\help\License_Administration.htm where *PMP directory* is the PMP directory on the server where PMP is installed.

- **Configuration.** Enables you to monitor the performance of selected servers, as well as change the monitoring parameters of the monitored servers.

To access **Configuration**, select **Options->Performance Management Pack Options->Configuration**.

To access help for this option, go to

https://middle_tier:2381/pmp/help/Monitoring_Administration.htm where *middle_tier* is the name or IP address of the server that HP SIM and PMP are installed, or access *PMP directory*\Program Files\HP\Performance Management Pack\PMP\htm\help\Monitoring_Administration.htm where *PMP directory* is the PMP directory on the server where PMP is installed.

- **Manual Log Purge.** Enables you to delete the unwanted or past logged data from the PMP repository.

To access **Manual Log Purge**, select **Options->Performance Management Pack Options->Manual Log Purge**.

To access help for this option, go to

https://middle_tier:2381/pmptools/help/ManualLogPurge.htm where *middle_tier* is the name or IP address of the server that HP SIM and PMP are installed, or access *PMP directory*\Program Files\HP\Performance Management Pack\PMPTools\htm\help\ManualLogPurge.htm where *PMP directory* is the PMP directory on the server where PMP is installed.

Related Topics

- PMP Tools
- PMP Reporting Options

Setting Up Managed Systems

Overview

Setting up managed systems involves installing the required management agents and configuring the supported protocols to communicate with the HP Systems Insight Manager software. The following steps assume that HP Systems Insight Manager is installed on the central management server (CMS) and the First Time Wizard has been completed.

Note:



Discovery must be run prior to setting up managed systems. Refer to “Running a Discovery Task” for more information. Configuring Automatic Discovery is part of the First Time Wizard.

To setup managed systems, there are two overall steps:

1. Installing required and optional managed system software:
 - “Installing the ProLiant Support Pack on Windows systems for the first time”
 - “Installing the ProLiant or Integrity Support Pack on a Linux system for the first time”
 - “Installing the required software on an HP-UX system”
2. Configuring the managed system software:
 - “Run the Configure or Repair Agents feature from the CMS”

Installing Required and Optional managed system software

Managed systems must have the VCA installed prior to using the Configure or Repair Agents feature to configure them.

Installing the ProLiant Support Pack on Windows systems for the first time

For Windows systems, install the latest ProLiant Support Pack with the preconfigured components to all managed systems using the HP Systems Insight Manager feature **Initial ProLiant Support Pack Install**.

When you are installing the ProLiant Support Pack for the first time, the Initial ProLiant Support Pack Install process enables you to install a ProLiant Support Pack to a Windows system because you do not have any HP Insight Management Agent, especially HP Version Control Agent, installed. This process also configures the systems to use the trust certificate from the HP Systems Insight Manager and the setting to use the desired HP Version Control Repository Manager. After you have run the Initial ProLiant Support Pack Install tool, then you can use the Install Software and Firmware tool to update systems.

The Install Software and Firmware feature in HP Systems Insight Manager requires that the HP Version Control Repository Manager be installed on servers containing a repository. Installing the VCRM is not part of this procedure. For more information regarding installing the VCRM, refer to the HP Version Control Installation Guide at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

Note:



You must have Windows administrator privileges on target systems to install a ProLiant Support Pack

Note:



The Install Software and Firmware and VCA features are only available after the Initial ProLiant Support Pack Install process has been run.

Note:



For more information regarding ProLiant Support Packs, refer to the *HP ProLiant Support Pack and Deployment Utilities User Guide* at <http://h18013.www1.hp.com/manage/psp.html>.

To install a ProLiant Support Pack:

1. Select **Deploy>Deploy Drivers, Firmware and Agents>Initial ProLiant Support Pack Install**. The **Initial ProLiant Support Pack Install** page appears.
2. Select the target systems. Refer to “Managing with Tasks” for more information.
3. Click **Next**.
4. From the **Enter Windows login credentials** page:
 - a. In the **User name** field, enter the Windows administrator user name for the target system.
 - b. In the **Password** field, enter the administrator password for the Windows user name entered above.
 - c. In the **Password (Verify)** field, reenter the Windows administrator password exactly as it was entered in the **Password** field.
 - d. In the **Domain** field, enter the Windows domain.
Note: This field can be left blank if the system is not part of a domain.
5. Click **Next**. The **Select a Windows Support Pack** page appears.
6. Under **Select a Version Control Repository**, select a source repository system from which to retrieve the catalog.

The following fields display:

- **Name**. This field displays the name of the system.
- **Status**. This field displays the status of the system.
- **Product Name**. This field displays the name of the product.
- **Trusted?**. This field indicates whether the system trust relationship has been configured. To configure a trust relationship, click **configure**. Refer to “Trusted Certificates” for more information.

Note: This section displays systems that are authorized by the current user name. If the current user is not authorized to view the systems, a message appears, indicating that the user does not have authorization rights on the system.

7. Under **Select a Support Pack to Install**, select a support pack to install. Click the  icon to drill down and view the contents of the Version Control Repository that you selected.
Note: To expand the **System Software Baseline** to display all contents, click the  icon located in the upper left corner of the **Select a Support Pack to Install** section. Click the  icon to collapse the listings.
8. Select **Install and initialize SSH (Secure Shell)** if you want to install and configure OpenSSH on the target systems. This option is disabled by default.

9. (Optional) Select **Force downgrade or re-install the same version** if you are installing a ProLiant Support Pack that is older than or the same as the version currently installed. This option is disabled by default.
10. By default, **Reboot systems if necessary after successful install** is selected. You can deselect this option if you do not want to reboot after the installation. However, the system must be rebooted for the new ProLiant Support Pack to be available.
11. Click **Next**. The **Configure Support Pack** page appears.

- If you select a ProLiant Support Pack 7.10, **Configure a Support Pack** appears. For example:

Note: If you select a ProLiant Support Pack that is earlier than 7.10, the following example varies.

To configure the 7.10 support pack:

- a. Click **Configure Support Pack** to set up the HP Version Control Agent in the selected Support Pack. The **VCA Setup** page appears.
Note: If the VCA has already been configured, you can omit this step.
- b. In the **Computer Name** field, enter the name of the system where the VCRM is installed.
- c. In the **Administrator Password** field, enter the password associated with the login name specified.
- d. Click **Save** to save your settings. Click **Cancel** to discard your settings and close the **VCA Setup** page.
- e. Click **Next**. The **Download Support Pack** page appears.
- f. After the support pack is downloaded, click **Schedule** to create a scheduled task for the Initial ProLiant Support Pack Install to run or click **Run Now** to run the task immediately.

If you select a ProLiant Support Pack 7.20 or later, the following options display.

- Click **Configure System Management Homepage** to setup the Support Pack to establish a trust relationship with System Management Homepage when it is installed on target systems.

Note: If the Support Pack has already been configured, you can skip this step.

Note: Refer to "Trusted Certificates" for more information on setting up a trust relationship. the trust relationship is established, click **Last Update** to update the status to trusted.

To configure the System Management Homepage:

- a. From the **Welcome to the Configuration Wizard for the HP System Management Homepage Component** page, click **Next**. The **Operating Systems Groups** page appears.
- b. In the **Group Name** field, enter the name of an operating system group that you want to assign. For example, *vcadmin*.

- c. In the **Operating Level** field, select the appropriate level for the new group from the dropdown list.

Note: The default **Administrators Groups** always have administrative access.

- d. Click **Add** to assign the group. The new group appears under the operating system group which it was assigned.

Note: You can add up to five entries per operating system group.

- e. Click **Next**. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.

- f. **Local** and **Anonymous** access enables you to select the appropriate settings to include:

- Anonymous Access.** Anonymous Access is disabled by default. Enabling **Anonymous Access** enables a user to access the System Management Homepage (SMH) without logging in. Select this option to allow anonymous access.

Caution: HP does not recommend the use of anonymous access.

- Local Access.** Local Access is disabled by default. Enabling it means you can locally gain access to the System Management Homepage without being challenged for authentication. This means that any user with access to the local console is granted full access if **Administrator** is selected. If **Anonymous** is selected, any local user has access limited to unsecured pages without being challenged for a username and password. Select this option to allow local access.

Caution: HP does not recommend the use of local access unless your management server software enables it.

- g. Click **Next**. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.

- h. The **Trust Mode** options enable you to select the security required by your system. There are some situations that require a higher level of security than others. Therefore, you are given the following security options:

- Trust by Certificate.** Sets the System Management Homepage (SMH) to accept configuration changes only from HP Systems Insight Manager servers with trusted certificates. This mode requires the submitted server to provide authentication by means of certificates. This mode is the strongest method of security since it requires certificate data and verifies the digital signature before allowing access. If you do not want to enable any remote configuration changes, leave **Trust by Certificate** selected, and leave the list of trusted systems empty by avoiding importing any certificates.

Note:



HP strongly recommends using this option as it is more secure.

To trust by certificate:

1. Select **Trust by Certificate** and click **Next**.
 2. In the **Certificate Name** field, click **Browse** to select the certificate file. After the certificate file is selected, the certificate data is displayed on the screen.
 3. Click **Add**. The certificate appears under **Certificate Files**. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.
 4. Click **Next**. The **IP Binding** page appears.
- Trust by Name.** Sets the System Management Homepage to accept certain configuration changes only from servers with the HP Systems Insight Manager names designated in the **Trust By Name** field. The **Trust By Name** option is easy to configure. For example, you might use the trust by name option if you have a secure network with two separate groups of administrators in two separate divisions. It prevents one group from installing software to the wrong system. This option verifies only the HP Systems Insight Manager server name submitted.

Note:



HP strongly recommends using the **Trust by Certificate** option as the other options are less secure.

The server name option must meet the following criteria:

- Each server name must be less than 64 characters
- The overall length of the server name list is 1,024 characters
- Special characters should not be included as part of the *server name*: ~ ' ! @ # \$ % ^ & * () + = \ " : ' < > ? , |
- Semicolons are used to separate *server names*

To trust by name:

1. Select **Trust by Name** and click **Next**.

2. In the **Trusted Server Name** field, enter the server name to be trusted.
 3. Click **Add**. The trusted system name appears under the **Trusted Servers** list. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.
 4. Click **Next**. The **IP Binding** page appears.
- Trust All.** Sets the System Management Homepage to accept certain configuration changes from any system.

Note:



HP strongly recommends using the **Trust by Certificate** option as the other options are less secure.

To trust all servers:

1. Select **Trust All**. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.
 2. Click **Next**. The **IP Binding** page appears.
- i. IP Binding specifies from which IP addresses the System Management Homepage (SMH) accepts requests from and provides control over which nets and subnets requests are processed.

Administrators can configure the System Management Homepage to only bind to addresses specified in the **IP Binding** page. A maximum of five subnet IP addresses and netmasks can be defined.

An IP address on the server is bound if it matches one of the entered IP Binding addresses after the mask is applied.

Note:



The System Management Homepage always binds to 127.0.0.1. If IP Binding is enabled and no subnet/mask pairs are configured, then the System Management Homepage is only available to 127.0.0.1. If IP Binding is not enabled, you bind to all addresses.

To configure IP Binding:

1. Select **IP Binding**. The **IP Binding** page appears.

2. Enter the IP address.
 3. Enter the Netmask.
 4. Click **Add**. The IP binding configuration is saved and appears under the **IP Binding List**.
 5. Click **Next**. The **IP Restricted Login** page appears.
- j. The IP Restricted Login enables the System Management Homepage (SMH) to restrict log-in access based on the IP address of a system.

You can set address restriction at installation time or by it can be set by administrators from the **IP Restricted Login** page

- If an IP address is excluded, it is excluded even if it is also listed in the included box.
- If there are IP addresses in the inclusion list, then only those IP addresses are allowed log-in access with the exception of *localhost*.
- If no IP addresses are in the inclusion list, then log-in access is allowed to any IP addresses not in the exclusion list.

To include or exclude IP addresses:

1. In the **From** field, enter the IP addresses to include or exclude. You can enter an IP address range to be included or excluded by entering a beginning IP address in the **From** field and an ending IP address in the **To** field.
 2. From the **Type** field, select **Include** or **Exclude**.
 3. Click **Add** to add the IP address or IP address range to the **Inclusion List** or **Exclusion List** below.
 4. Click **Save**. The **HP System Management Homepage Login** page for the System Management Homepage system appears. For more information about System Management Homepage, refer to the System Management Homepage Online Help at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.
- Click **Configure VCA** to set up the HP Version Control Agent in the selected Support Pack.

Note: If the VCA has already been configured, you can skip this step.

To configure the VCA:

- a. In the **Computer Name** field, enter the name of the system where the VCRM is installed.
- b. In the **Login Account** field, enter the login name used to connect to the VCRM on the system specified.

- c. In the **Login Password** field, enter the password associated with the login name specified.
 - d. Click **Save** to save your settings. Click **Cancel** to discard your settings and close the **VCA Setup** page.
 - e. Click **Next**.
12. Back in HP Systems Insight Manager, click **Next** to start the ProLiant Support Pack download. The **Download Support Pack** page appears.
 13. After the support pack is downloaded, click **Schedule** to create a scheduled task for the Initial ProLiant Support Pack Install to run or click **Run Now** to run the task immediately.

Installing the ProLiant or Integrity Support Pack on a Linux system for the first time

- For Linux systems, use the Linux Deployment Utility to install the latest support pack with the preconfigured components to the local system. For more information regarding installing a support pack using the Linux Deployment Utility, refer to <http://www.hp.com/servers/psp>.

Installing the required software on an HP-UX system

1. Understanding the basic managed system software for HP-UX.

For HP-UX, the following software, shown with minimum recommended versions, is required for essential HP Systems Insight Manager functionality to operate. This software is installed by default as part of the latest HP-UX 11i v2 operating environments, but may need to be installed or updated on HP-UX 11i v1 or older HP-UX 11i v2 systems.

- T1471AA A.04.00 HP-UX Secure Shell
- B8465BA A.02.00.05 HP WBEM Services for HP-UX

This WBEM Services bundle contains basic system instrumentation displayed in the HP SIM Property Pages as well as supporting collection and reporting by HP SIM Inventory functionality. To maximize the value of SIM for properties, inventory and events, the following should also be installed, available for HP-UX 11i v2 servers:

- LVMProvider R11.23 CIM/WBEM Provider for LVM
- WBEMP-LAN-00 B.11.23 LAN Provider for Ethernet/LAN Interfaces
- SysFaultMgmt A.02.00 HP-UX System Fault Management

The following, System Management Homepage for HP-UX, does not currently support the same level of functionality found in Windows and Linux servers. It is currently only required to support the latest version of Partition Manager.

- SysMgmtWeb A.2.2 HP-UX Web Based System Management User Interfaces

2. Ensuring the managed system software is installed

To see if the minimum required software is installed, login to the remote system and run the following command:

```
$ swlist -l bundle T1471AA B8465BA OpenSSL
```

To see if the optional providers and System Management Homepage are installed, run commands such as:

```
$ swlist -l bundle LVMPProvider WBEMP-LAN-00 SysFaultMgmt
```

3. Acquiring and Installing managed system software

The SecureShell, WBEM and OpenSSL bundles are included on the HP-UX Operating Environment and Application Release media, as well as part of the HP Systems Insight Manager HP-UX depot downloaded from <http://www.hp.com/go/softwaredepot>.

For the WBEM providers, several are available from the latest HP-UX Operating Environment and Application Release media. Additionally, the LVMprovider and SysFaultMgmt are available from <http://www.hp.com/go/softwaredepot> by searching for the keyword *provider*.

Make sure that the OnlineDiag bundle is installed on your computer.

To verify that the OnlineDiag bundle is installed, enter the following command:

```
swlist | grep OnlineDiag
```

The OnlineDiag bundle is installed on the operating environments, so if you have a recent version of the operating environment, this should already be installed. However, if it is not installed, the OnlineDiagnostic bundle is available from <http://www.hp.com/go/softwaredepot> by searching for the keyword *B6191AAE*.

After the depots containing the providers have been acquired, they can be installed from the managed system using commands such as:

```
$ swinstall -s <depot_location> OpenSSL
```

Note:B8465BA depends on OpenSSL, so this must be installed first.

```
$ swinstall -s <depot_location> T1477AA
```

```
$ swinstall -s <depot_location> B8465BA
```

```
$ swinstall -s <depot_location> LVMPProvider WBEMP-LAN-00 SysFaultMgmt
```

4. Configuring Serviceguard provider:

A WBEM provider for Serviceguard can be optionally installed on HP Serviceguard clusters. This provider helps HP Systems Insight Manager create associations in its system lists between clusters and their members, as well as showing HP Serviceguard cluster status.

When using the First Time Wizard from HP Systems Insight Manager, the root user or a non-root user was specified for the WBEM default user. Alternatively a user may have been specifically set for this system.

To access the Serviceguard provider from HP Systems Insight Manager if a non-root user is the WBEM user, you must configure Serviceguard to allow that non-root user Serviceguard

administrative access. Refer to “HP Serviceguard Manager Overview” for more information about ServiceGuard.

Configuring the Managed System Software

The HP Systems Insight Manager Configure or Repair Agents feature is a quick and easy way to configure managed systems, however it is possible to manually configure Linux and HP-UX systems.

Run the Configure or Repair Agents feature from the CMS

To run Configure or Repair Agents remotely against multiple systems simultaneously, you must have authorizations to run the Configure or Repair Agents tool.

You must have full CMS configuration privileges to modify the HP Systems Insight Manager community strings in the node security file. In addition, you must have administrator privileges for Windows systems or root privileges for Linux and HP-UX on the target systems to configure or repair the agent settings.

Note: It is recommended that you use like operating system to configure a managed system. For example, use a Linux-based CMS to run Configure or Repair Agents against Linux managed systems and HP-UX CMS to run Configure or Repair Agents against HP-UX managed systems. Windows systems can only be configured from a Windows CMS.

To configure agents remotely:

1. Select **Configure->Configure or Repair Agents** from the menu.

Note: The **Verify Target Systems** page appears if the targets are selected before selecting a tool.

2. To add targets, select a group from the dropdown list. The contents of the selected group appear and can be selected as targets or to select the collection itself, select **Select Name of Collection itself**.
3. Click **Apply**.The targets appear in the **Verify Target Systems** section.

Note: If the targets selected are not compatible with the tool, the **Tool Launch OK?** column provides a brief explanation for the problem. To remove a target, select the target and then click **Remove Targets**.

4. Select one of the following options:
 - Click **Add Targets** to add more targets to the **Target System List**.
 - To remove a target, select the target and then click **Run Targets**.
 - Click **Next** to specify tool parameters and to schedule the task.
5. From the **Enter login credentials** page:
 - a. In the **User name** field, enter the system administrator user name for the target systems.
 - b. In the **Password** field, enter the system administrator password for the user name previously entered.

- c. In the **Password (Verify)** field, reenter the system administrator password exactly as it was entered in the **Password** field.
- d. For Windows managed systems only, in the **Domain** field, enter the Windows domain.

Note: The credentials used in this step must work for all target systems that have been selected. HP recommends using domain **administrator** or **root** credentials.

6. Click **Next**. Click **Prev** to return to the previous page. The **Configure or Repair Settings** page appears.

The following options are available:

- **Configure SNMP.** Select this option to configure SNMP settings.

If this option is selected, the following steps must be considered:

1. Select **Set read community string**.

Note: If only HP-UX systems with default SNMP installation are being configured at this time, you may deselect this option. HP-UX allows read by default (get-community-name is set to public by default on HP-UX systems).

Note: If this option is selected, the **Read Only** community string is added to the target systems. If the target system is SuSE Linux or Microsoft Windows 2003, the managed nodes do not always allow SNMP communication between themselves and a remote host. This setting is modified to allow the instance of the HP Systems Insight Manager system to communicate SNMP with these target systems.

Note: Repairing the SNMP settings adds a **Read Write** community string to the target system only if one does not currently exist. This community string is unique for each system, is composed of over thirty characters to include letters and numbers, and is only visible to the user with administrator privileges for that system. This **Read Write** community string is required by the Web Agent to perform certain threshold setting capabilities. This community string is only used locally on the target system and is not used by HP Systems Insight Manager over the network.

2. Select **Set traps to refer to this instance of HP Systems Insight Manager** in the target systems' **SNMP Trap Destination List**. This allows the target systems to send SNMP traps to this instance of HP Systems Insight Manager.

- **Trust relationship: Set to "Trust by Certificate".** Select this option to require systems to use the **Trust by Certificate** trust relationship with the System Management Homepage.

For System Management Homepage on the target systems, this option sets the trust mode to **Trust by Certificate** and copies the HP Systems Insight Manager system certificate to the target system's trusted certificate directory. This enables HP Systems Insight Manager users to connect to the System Management Homepage using the certificate for authentication.

Note: If you experience problems later setting the trust status to Linux, refer to the HP Systems Insight Manager Online Help **Troubleshooting** help file for assistance.

- **Set administrator password for Insight Management Agents version 7.1 or earlier.** Select this option to repair the administrator password on all Insight Management Agents installed on the target systems as applicable for Windows and Linux systems.

Note: Deselect this option if you have Insight Management Agents 7.2 or later installed.

Note: If the remote system is running HP-UX, this option is not executed on the remote system since it is not applicable on HP-UX systems. If only HP-UX target systems are being configured at this time, you can deselect this option.

If this option is selected, the following steps must be configured:

1. In the **Password** field, enter the new administrator password.
2. In the **Confirm Password** field, re-enter the new administrator password exactly as you entered it previously.

- **Configure secure shell (SSH) access.**

If this option is selected, you must select one of the following options:

- **Host based authentication for SSH** - For more information regarding SSH, refer to Secure Shell (SSH) in HP Systems Insight Manager white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Each user has to be authenticated on the managed system**

Note: If the selected systems include Linux or HP-UX systems, and options for Configure SNMP settings, Trust relationships and administrator password for HP Insight Management Agent 7.1 or earlier have been selected, then SSH authentication should be selected now unless already configured earlier.

Note: SSH can be configured only if the OpenSSH service is running on the managed systems. OpenSSH can be installed on Windows systems, by running the **Install Open SSH** tool under **Deploy->Deploy Drivers, Firmware and Agents->Install Open SSH**.

- **Create subscriptions for WBEM events.**

Note: This option is only applicable to Linux and HP-UX systems. If this option is selected, the target system is configured to send WBEM indications or events to HP Systems Insight Manager.

Note: Subscriptions for WBEM events can be created only if WBEM event providers are installed and running on the managed systems.

7. Click **Run Now** or you can click **Schedule** to run this task at a later time. Click **Prev** to return to the previous page. The **Task Results** page appears.

Note: The Configure or Repair Agents tool can be used to update multiple target systems, each of which might potentially have different results. The information is used to display the information on the stdout tab. The results indicate whether the repair attempt was successful.

Note: Repair of SNMP settings, Trust relationships and administrator password for Insight Management Agents 7.1 or earlier on Linux systems is executed by a separate task, which can be viewed in the tasks log menu selection. Repair of SNMP settings, Trust relationships on HP-UX systems is executed by a separate task, which can be viewed in the tasks log menu selection. If Linux and HP-UX systems are selected, there are two Task IDs, one for Linux and one for HP-UX systems.

The **Task Results** page displays the following information:

- **Status.** This field displays the details for each target system within a task instance.
- **Exit Code.** This field represents the success or failure of an executable program. If the return value is zero or positive, the executable ran successfully. If a negative value is returned, the executable failed.
- **Target Name.** This field displays the name/IP address of the target.
- **The stdout Tab.** This tab displays the output text information.
- **The stderr Tab.** This tab displays information if the executable experienced an error.
- **Files Copied Tab.** This tab displays what files are in the process of being copied or have been copied to the target system.
- **View Printable Report.** Reports can be printed for the currently selected target system or for all target systems associated with the task instance.

To print a report:

1. Click **View Printable Report**.

An **Options Message** box appears, asking if you want to generate a report containing only the currently selected target system or all systems associated with the task instance.

2. Select which report to print.
3. Click **OK** to print the report, or click **Cancel** to return to the **View Task Results** page.

8. If Management HTTP Server is installed on target systems, the login credentials are updated in the Management HTTP Server password file.

Setting Up Managed Systems Manually

Using HP Systems Insight Manager's Configure or Repair Agents is the easiest way to configure managed systems. However, the steps to manually configure Linux and HP-UX managed systems are included in the event manual configuration is necessary.

The following sections detail how to configure managed systems on:

- "Setting Up HP-UX Managed Systems Manually"
- "Setting Up Linux Managed Systems Manually"

Setting Up HP-UX Managed Systems Manually

You can use the HP Systems Insight Manager Configure or Repair Agents tool to configure HP-UX managed systems simultaneously or you can configure each managed system manually.

Use these general steps to assist you with configuring an HP-UX system manually:

1. Install SSH (bundle T1471AA) if not previously installed.
2. Install WBEM (bundle B8465BA) if not previously installed.
3. (Optional) Configure SNMP to send traps to the CMS.
4. (Optional) Configure DMI on HPUX 11.11 systems (this step is not needed if WBEM installed).

On the CMS:

5. Configure the SSH Keys for this system.
6. Configure the default WBEM user name and password if not previously done.

Note:



SSH and WBEM are installed on HPUX 11.23 systems by default. For 11.11 systems, check if installed with this command:

```
swlist B8465BA T1471AA
```

7. Subscribe to WBEM Indications/Events

On each managed system:

1. Install SSH on the managed system if not previously installed.

```
swinstall -s /directory/depot T1471AA
```

where `directory` is the path to the depot file and `depot` is the name of the depot file. For example:

```
swinstall -s /tmp/HPSIM_download.depot T1471AA
```

2. Install WBEM on the managed system if not previously installed.

```
swinstall -s /directory/depot B8465BA
```

where `directory` is the path to the depot file and `depot` is the name of the depot file. For example:

```
swinstall -s /tmp/HPSIM_download.depot B8465BA
```

3. Configure SNMP to send traps to the CMS:

- a. Add the full hostname or IP address of the CMS as a trapdest in the following file:

```
/etc/SnmpAgent.d/snmpd.conf
```

trap-dest: hostname_or_ip_address

- b. Stop the SNMP Master agent and all subagents with the command:

/sbin/init.d/SnmpMaster stop

- c. Restart the SNMP Master agent and all subagents with the command:

/usr/sbin/snmpd

4. Configure DMI on the managed system by adding the DNS host name of the CMS.

Note:



DMI only needs to be configured for HP-UX 11.11 and only if WBEM is not installed.

- a. Stop the DMI daemon on the managed system:

/sbin/init.d/Dmisp stop

- b. Edit `/var/dmi/dmiMachines` by adding the host name of the CMS to the end of this file. Save the file.

- c. Start the DMI daemon:

/sbin/init.d/Dmisp start

5. On the CMS, copy the SSH-generated public key from the CMS to the managed system using the **mxagentconfig**:

Use one of the following commands:

- **mxagentconfig -a -n <hostname> -u root -f <file_with_root_password>**

or

- **mxagentconfig -a -n <hostname> -u root -p <root_password>**

Note: Using the `-p` option exposes the password through `ps` output, so use of the `-f` option (with a file only readable by root, and containing only the managed system root password) is highly recommended when using **mxagentconfig -a**. If the `-p` option is used, enclose the password in single quotes if the password has any special characters, such as `&` or `$`. For more information and options, see the **mxagentconfig** manpage with **man mxagentconfig**.

6. Log into the HP Systems Insight Manager GUI. For assistance with this, refer to “Signing In”. Using the GUI, add the default WBEM user name and password to the **Global Protocol Settings** page.

Note: An account for at least one of the WBEM user name and password combinations must exist on each managed system.

Note: This step can be performed once for all the managed systems you are setting up.

- a. Select **Options>Protocol Settings>Global Protocol Settings**.
- b. In the **Default WBEM settings** section, ensure that the **Enable WBEM** checkbox is selected, and add the default WBEM user name, password, and confirmation password.
- c. Click **OK**.

Note:



An account for at least one of the WBEM user name and password combinations must exist on each managed system. If the user in the Global Protocol Settings does not exist on the managed node you can set per-system WBEM user names and passwords from the **System Protocol Settings** page.

7. To subscribe to WBEM Indications/Events:

Note: For more information about OnlineDiagnostic, go to WBEM Subscriptions in HP Systems Insight Manager white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- a. From the managed system, make sure WBEM is already installed.

Note: Subscribing to WBEM Indications/Events on managed systems is optional.

- b. Verify that **SysFaultMgmt** provider is installed:

```
cimprovider -ls
```

You should see **EMSWrapperProviderModule**

From the CMS:

1. Verify that WBEM has root access:

```
mxnodesecurity -l -p wbem -n <systemname>
```

To subscribe to WBEM Events, you must have **root** access. If the Global Protocol Setting does not match the managed system or does not contain **root** access, the subscription for WBEM Indications fails. You can verify what access WBEM has by running the following command line:

```
mxnodesecurity -l -p wbem -n <systemname>
```

If the managed system does not have **root** access, you can change the individual system.

Note: You can use the Configure or Repair Agents tool to perform this step without permanently recording a **root** passwd.

To change the individual system:

- a. **Tools->System Information->System Page.**
 - b. From the **System Page**, select **Tools & Settings->System Protocol Settings.**
2. From the CMS, run the WBEM Indications/Events command line:

```
mxwbemsub -l -n <systemname>
```

Refer to “Subscribing to WBEM Indications” for more information.

Setting Up Linux Managed Systems Manually

You can use the HP Systems Insight Manager Configure or Repair Agents tool to configure Linux managed systems simultaneously or you can configure each managed system manually.

To manually configure Linux managed systems, perform the following on each managed system:

1. Install and configure SSH.
 - a. Verify that SSH is installed on the managed system:

```
rpm -qa | grep ssh
```

If it is not installed, refer to your Linux provider for information on installing SSH.
 - b. On the CMS, copy the SSH generated public key from the CMS to the managed system and place it in the authorized keys file of the execute-as user (root or administrator).

Important: On a non-English CMS, ensure that an administrator account (spelled exactly as follows, administrator) exists on the CMS, and that **mxagentconfig** has been run on the CMS for the created administrator account.

 - i. Launch the **Manage SSH Keys** dialog box from the CMS command prompt:

```
mxagentconfig -a -n hostname -u username -p Password
```
 - ii. Click **Connect**.
2. Configure the system to send SNMP traps.

Note: These steps might vary slightly, depending on your version of Linux. Refer to your Linux provider for details if these file paths and file names do not exist on your system.

 - a. Verify that SNMP is installed:

```
rpm -qa | grep snmp
```

If it is not installed, refer to your Linux provider for information on installing SNMP.
 - b. If you have not installed the HP Server Management Drivers and Agents from the ProLiant Support Pack for Linux, omit this step. Otherwise, stop the HP Server and Management

Drivers and Agents daemons on the platform where you are installing HP Systems Insight Manager using the following command:

```
/etc/init.d/hpasm stop
```

Note: If the HP Server Management Drivers and Agents daemon is not installed, omit this step and step F.

- c. Stop the SNMP daemon:

```
/etc/init.d/snmpd stop
```

- d. Edit the `snmpd.conf` file using any text editor.

For Red Hat Linux run the following command for opening this file in the vi editor: **vi /etc/snmp/snmpd.conf**

For SuSE SLES 8 run the following command for opening this file in the vi editor: **vi /usr/share/snmp/snmpd.conf**

- i. Remove the comment symbol (#) from the `trapsink` line, and add the IP address of the CMS:

```
trapsink IPaddress
```

where *IPaddress* is the IP address of the CMS.

- ii. Add the CMS to the read only community by adding the line:

```
rocommunity CommunityName IPaddress
```

where *CommunityName* is the SNMP community string used by the CMS and *IPaddress* is the IP address of the CMS.

- iii. Save the changes to the file. To save and close this file using the vi editor, press the Esc key, enter **:wq!**, and press the Enter key.

- e. Start the SNMP daemon:

```
/etc/init.d/snmpd start
```

- f. Start the HP Server Management Drivers and Agents daemon if it is installed on your system:

```
/etc/init.d/hpasm start
```

3. Install the Linux ProLiant Support Pack. To download this software and access installation information, go to <http://www.hp.com/support/files>.
4. Log into the HP Systems Insight Manager GUI. For assistance with this, refer to "Signing In".
5. Add the default WBEM user name and password to the **Global Protocol Settings** page in the HP Systems Insight Manager GUI.

Note: An account for at least one of the WBEM user name and password combinations must exist on each managed system.

Note: This step can be performed once for all the managed systems you are setting up.

- a. Select **Options>Protocol Settings>Global Protocol Settings**.
- b. In the **Default WBEM settings** section, ensure that the **Enable WBEM** checkbox is selected, and add the default WBEM user name, password, and confirmation password.
- c. Click **OK**.

Examples

Setting up Windows managed systems

The following example describes how to setup remote Windows systems from a Windows CMS.

To configure remote Windows systems from a Windows CMS:

1. Login to the HP Systems Insight Manager on the Windows CMS with full CMS configuration privileges.
2. Run the First Time Wizard if you have not already. Refer to “Running a Discovery Task” for more information.
3. Run discovery if you have not already. Refer to “First Time Wizard” for more information about running the First Time Wizard.
4. Preconfigure the System Management Homepage and version control components.
5. Install the ProLiant or Integrity Support Packs on remote systems:
 - Run the Initial ProLiant Support Pack Install to install the latest ProLiant Support Pack on Windows systems. For details, refer to “Installing the ProLiant Support Pack on Windows systems for the first time”.
6. Run the Configure or Repair Agents feature. For more information, refer to “Run the Configure or Repair Agents feature from the CMS”.

Setting up remote Linux systems from a Linux CMS

The following example describes how to setup remote Linux systems from a Linux CMS.

To configure remote Linux systems from a Linux CMS:

1. Login to the HP Systems Insight Manager on the Linux CMS with full CMS configuration privileges.
2. Run the First Time Wizard if you have not already. Refer to “Running a Discovery Task” for more information.
3. Run discovery if you have not already. Refer to “First Time Wizard” for more information about running the First Time Wizard.

4. Preconfigure the System Management Homepage and version control components.
5. Install the ProLiant or Integrity Support Packs on remote systems:
 - Run the Linux Deployment Utility to install the latest Integrity Support Pack on Linux and HP-UX systems. For more information, download the HP ProLiant Support Pack and Deployment Utilities User Guide at <http://www.hp.com/servers/psp>.
6. Run the Configure or Repair Agents feature. For more information, refer to “Run the Configure or Repair Agents feature from the CMS”.

Setting up remote HP-UX systems from an HP-UX CMS

The following example describes how to set up remote HP-UX systems from an HP-UX CMS.

To configure remote HP-UX systems from an HP-UX CMS:

1. Login to the HP Systems Insight Manager on the HP-UX with full CMS configuration privileges.
2. Run the First Time Wizard if you have not already. Refer to “Running a Discovery Task” for more information.
3. Run discovery if you have not already. Refer to “First Time Wizard” for more information about running the First Time Wizard.
4. Ensure the managed system software is installed. For more information, refer to “Installing the required software on an HP-UX system”.
5. Run the Configure or Repair Agents feature to configure the managed system. For more information, refer to “Run the Configure or Repair Agents feature from the CMS”.

Related Topics

- Setting Up Trust Relationships
- Version Control

Managing SSH Keys

The **SSH Keys** feature enables you to view and manage the public Secure Shell (SSH) keys, stored in the `known_hosts` file, from the central management server (CMS). SSH keys enable the CMS and a managed system to authenticate a secure connection.

HP Systems Insight Manager (HP SIM) provides the following SSH key configuration options:

- **Select secure shell public keys security level.** Select **Options->Security->SSH Keys**.
- **Import SSH keys.** Select **Options->Security->SSH Keys**, select the SSH Key to be imported, and click **Import**.
- **Export SSH keys.** Select **Options->Security->SSH Keys**, select the SSH Key to be exported, and click **Export**.

- **Delete SSH keys.** Select **Options->Security->SSH Keys**, select the SSH Key to be deleted, and click **Delete**.

Related Procedures

- Importing an SSH Key
- Exporting an SSH Key
- Deleting an SSH Key
- Configuring SSH Key Security

Configuring SSH Key Security

Configuring the Secure Shell (SSH) key security level enables you to specify the level of security on the central management server (CMS).

To configure the SSH key security level on the CMS:

1. Select **Options->Security->SSH Keys**. The **SSH Keys** page appears.

Under **Select managed systems SSH public key behavior**, the following options are available:

- **The central management server saves the key sent the first time an SSH connection is made.**
- **The central management server accepts an SSH connection with any key, even if not in the list below.**

This option is selected by default.

This option causes all connections to the host to be accepted, even when the SSH key has changed. The `known_hosts` file is disabled and updated to reflect the new key.

Note: This option provides no protection against man-in-middle attacks.

- **The central management server accepts an SSH connection only if the key is in the list below**

This option requires the SSH key to appear in the **Managed Systems SSH Public Keys** list.

Note: HP recommends this option because it is the most secure.

2. Click **OK**. The setting is saved.

Related Procedures

- Importing an SSH Key
- Exporting an SSH Key
- Deleting an SSH Key

Related Topic

- Managing SSH Keys

Importing an SSH Key

Importing a Secure Shell (SSH) key list enables the central management server (CMS) to authenticate a secure connection and execute commands on managed systems. Multiple SSH keys are imported from one file and each SSH key appears on a line and is associated with a host system.

Note:



Only correctly formatted SSH keys can be imported into the Managed Systems SSH public keys list.

Refer to the *Secure Shell (SSH) in HP Systems Insight Manager 5.0* white paper located at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information on the format of the SSH keys file.

To import an SSH key on the CMS:

1. Select **Options->Security->SSH Keys**. The **SSH Keys** page appears.
2. Click **Import**. The **Import SSH Keys** section appears under the **Managed Systems SSH Public Keys** list.
3. Click **Browse** to navigate to the file that contains the SSH keys to be imported.
4. Select the file and click **Open** to add the key to the **Managed Systems SSH Public Keys** list, or click **Cancel** to abort the operation.

Related Procedures

- Exporting an SSH Key
- Deleting an SSH Key
- Configuring SSH Key Security

Related Topic

- Managing SSH Keys

Exporting an SSH Key

Exporting selected Secure Shell (SSH) keys saves the SSH keys to a file. This file can be used to import the SSH keys into the SSH key list on other systems.

To export SSH keys on the central management server (CMS) to a file:

1. Select **Options->Security->SSH Keys**. The **SSH Keys** page appears.
2. From the **Managed Systems SSH Public Keys** list, select the SSH key to be exported. You can select **System** to select all SSH keys in the list.
3. Click **Export**. The **Export SSH Keys** section appears.

4. Right-click the link provided and select **Save Target As**. The **Save As** dialog box appears.
5. Navigate to the directory where you want to store the file.
6. Click **Save**. The key is exported.
7. Click **OK**.

Related Procedures

- Importing an SSH Key
- Deleting an SSH Key
- Configuring SSH Key Security

Related Topic

- Managing SSH Keys

Deleting an SSH Key

Deleting Secure Shell (SSH) keys from the **Managed Systems SSH Public Keys** list enables you to remove SSH trusted keys on the central management server (CMS).

To delete an SSH key on the CMS:

1. Select **Options->Security->SSH Keys**. The **SSH Keys** page appears.
2. From the **Managed Systems SSH Public Keys** list, select the SSH key to be deleted.
3. Click **Delete**. A message appears, indicating you are about to delete SSH keys.
4. Click **OK**. The key is removed from the **Managed Systems SSH Public Keys** list.

Related Procedures

- Importing an SSH Key
- Exporting an SSH Key
- Configuring SSH Key Security

Related Topic

- Managing SSH Keys

Backing Up and Restoring the Database

If you must reinstall HP Systems Insight Manager (HP SIM) but want to keep the information stored in the database, you must have a backup of the database. After the HP SIM reinstallation, you can restore the information from your previous database from the backup.

Related Procedures

- HP-UX/Linux
- Windows

Related Topics

- Reference Information

HP-UX/Linux

Backing up or Restoring the Database on the HP-UX or Linux Operating System

A PostgreSQL server database is used in HP Systems Insight Manager (HP SIM) to store all data relating to HP SIM. Back up your database regularly.

Use the PostgreSQL utilities to back up or restore the database:

- Use the `pg_dump` utility to back up the database.
- Use the `psql` utility to restore the database.

Note:



Refer to the manpages for these utilities for additional information.

Changing the HP SIM Database Password

During the HP SIM configuration, the **mxadmin** user is created in PostgreSQL, and the password is generated. You must change the password before you can use the `pg_dump` and `psql` utilities.

Enter `/opt/mx/bin/mxpassword -m -x MxDBUserPassword=newpassword` to change the HP SIM database password.

Related Procedure

- Windows

Related Topic

- Backing Up and Restoring the Database

Windows

A Microsoft SQL Server database (MSDE) is used by HP Systems Insight Manager (HP SIM) to store all collected information about the systems on your network as well as all configuration options. Always back up your database using an appropriate backup schedule. In the event of a catastrophic database problem, this backup can be restored to return HP SIM to operation.

If you must restore your database, stop the HP SIM Service from the Services applet before doing the restore. After the restore is complete, restart the service.

If you must reinstall HP SIM but want to preserve the information in your database, you must have a backup of your database. After reinstalling HP SIM, you can restore your previous database backup into the database created during the HP SIM installation.

Backing Up an SQL Server Database

Microsoft SQL Enterprise Manager has built in utilities to permit the database to be backed up. The backups can be automated if desired. HP also recommends viewing the help provided directly with SQL Enterprise Manager to gain a complete understanding of this procedure.

To backup the HP SIM database using Microsoft SQL Enterprise Manager:

1. Sign out of HP SIM, and stop the HP SIM Service.
2. Back up the configuration subdirectory *config* where HP SIM is installed.
Note: Use any tools that you are familiar with to back up a directory for this process. For example, you could use Windows Explorer to make a copy of the HP SIM installation directory.
3. Open Microsoft SQL Enterprise Manager using the **Start** menu from a Windows console.
4. In the tree displayed on the left side, expand the **Microsoft SQL Servers** branch and **SQL server** group. If the server where the HP SIM database is located is not listed, add it by selecting **New SQL Server Registration** from the right-click menu.
5. Select the server where the HP SIM database is located. From the **Tools** menu at the top, select **Backup database**. In the dialog that appears, select the database named *Insight_v**, and be sure that **Database-complete** is selected as the backup option.
6. Click **Add** in the destination, and select a location to backup the database. For example, a disk or tape.
7. Click **OK** to initiate the backup.

Restoring the SQL Server Database from a Backup

1. Open Microsoft SQL Enterprise Manager using the **Start** menu from a Windows console.
2. In the tree displayed on the left side, expand the **Microsoft SQL Servers** branch and **SQL server** group. If the server where the HP SIM database is located is not listed, add it by selecting **New SQL Server Registration** from the right-click menu.
3. Select the server where the HP SIM database is located. From the right-click menu at the top, select **All Tasks->Import Data**.
The DTS Import/Export Wizard launches. Click **Next**.
4. In the **Server** field, select the server where your exported database exists. Select **Windows Only** as the mode of authentication.
5. Select the name of the restored database from the **Database** dropdown list. For example, *Insight_v**.
6. Click **Next**.

7. Select your HP SIM system from the **Server** dropdown list. Select **Windows Only** as the mode of authentication. Select **Insight_v*** from the **Database** dropdown list. Click **Next**.
8. Select **Copy table(s) and view(s) from the source database**. Click **Next**.
9. Select **Select All buttons in the Select Source Tables and Views screen**. Click **Next**.
10. Select **Run Immediately**. Click **Next**.
11. Click **Finish**.
12. Click **Done**.
13. Restore the configuration subdirectory `config` where HP SIM is installed.
14. Start the HP SIM service.

Backing Up an MSDE Database

With MSDE, you can back up both data files and transaction logs. In the event of a failure, the most recent database backup is restored. When the restore is complete, you can apply the changes contained in all of the subsequent transaction log files, and the database is brought back to the state it existed when the last nightly transaction log was backed up.

If you have Microsoft Access 2000, you can use the **BACKUP** command in the **Database Utilities** menu of an Access project to back up an MSDE database. If SQL Client Tools are installed, you can use SQL Enterprise Manager to back up an MSDE database.

The SQL Client Tools and Access 2000 are not part of the Microsoft Data Engine (MSDE) install. Therefore, if you only have MSDE installed, you do not have the options associated with these programs. To back up an MSDE database, you can use the **TSQL BACKUP DATABASE** command and execute with **osql.exe** (command line Query tool). This procedure applies to Microsoft Data Engine (MSDE) 1.0. For information on all of the stored procedures in the following sections, refer to the SQL Books Online.

Backing Up HP SIM Using MSDE Command Line Features

1. Sign out of HP SIM, and stop the HP SIM service.
2. Back up the configuration subdirectory `config` where HP SIM is installed.
Note: Use any tools that you are familiar with to back up a directory for this process. For example, you could use Windows Explorer to make a copy of the HP SIM installation directory.
3. The following code is an example of how to use the various stored procedures with MSDE to perform a backup. This code does not back up your mission-critical database as is and might require some modification to run in your environment, such as changing your database name, server name, and so forth. Paste the following TSQL script in Notepad, and save it to a file called `myBackup.sql`:

```
--This TSQL script creates a backup job and calls sp_start_job to  
run the job.
```

```
--Create job.
--You may specify an e-mail address, commented below, and/or
  pager, etc.
--For more details on this option or others, reference SQL Books
  Online.
```

```
USE msdb
EXEC sp_add_job @job_name = 'mydbBackupJob',
  @enabled = 1,
  @description = 'mydbBackupJob',
  @owner_login_name = 'sa',
  @notify_level_eventlog = 2,
  @notify_level_email = 2,
  @notify_level_netsend =2,
  @notify_level_page = 2
```

```
-- @notify_email_operator_name = 'email name'
```

```
go
```

```
-- Add job step (backup data).
```

```
USE msdb
EXEC sp_add_jobstep @job_name = 'mydbBackupJob',
  @step_name = 'Backup INSIGHT Data',
  @subsystem = 'TSQL',
  @command = 'BACKUP DATABASE "Insight_v*" TO DISK
  =''c:\INSIGHT.dat_bak''',
  @on_success_action = 3,
  @retry_attempts = 5,
  @retry_interval = 5
```

```
go
```

```
-- Add job step (backup log).
```

```
USE msdb
EXEC sp_add_jobstep
  @job_name = 'mydbBackupJob',
  @step_name = 'Backup INSIGHT Log',
  @subsystem = 'TSQL',
  @command = <command> 'BACKUP LOG "Insight_v*" TO DISK' =
  'c:\INSIGHT.log_bak''',
  @on_success_action = 1,
  @retry_attempts = 5,
  @retry_interval = 5
```

```
go
```

```
--Add the target servers.
```

```
USE msdb
EXEC sp_add_jobserver @job_name = 'mydbBackupJob',
  @server_name = N'(local)'
```

```
-- Run job. Starts the job immediately.  
  
USE msdb  
EXEC sp_start_job @job_name = 'mydbBackupJob'  
  
-- The file has to be copied under /mssql/binn folder  
  
-- The command to execute it is OSQL -Smysqlserver  
  
-U sa -P password if any -i mybackup.sql -n
```

Related Procedure

- HP-UX/Linux

Related Topic

- Backing Up and Restoring the Database

Configuring SSH Bypass Properties

The `globalsettings.props` has many configurable properties. These settings are used to fine-tune the performance of various settings of HP Systems Insight Manager (HP SIM) to adjust to the running environment of the customer.

SSH Bypass is used to boost performance by bypassing the overhead of setting up SSH connections for specified users when the central management server (CMS) is executing a tool locally on the CMS. This also alleviates potential problems with SSH not being configured properly locally. This applies to tools that run exclusively on the CMS. This feature was introduced with HP SIM 4.2 SP2 – Windows and is also included for HP-UX and Linux with HP SIM 5.0. This feature is enabled by default for the root user on HP-UX and Linux, and for the administrator and the installer account on Windows.

To configure SSH bypass properties in `globalsettings.props`:

1. Open the `globalsettings.props` file located at:
 - **On Windows.** It is typically located at `C:\Program Files\HP\System Insight Manager\config\globalsettings.props`.
 - **On HP-UX and Linux.** It is located at `/etc/opt/mx/config/globalsettings.props`.
2. Edit the following properties:
 - **`mx_dtf_ssh_bypass_user`** . Modify this property to add additional user names for the SSH bypass feature. Separate each with a comma. For Windows domain accounts, two backslashes must exist between the domain name and the user name. For example,

`mydomain\myname`. You should not add a user name if you do not intend for them to have full administrator privileges on the CMS.

- **`mx_dtf_enable_ssh_bypass`** . Set this property to *True* to bypass use of SSH for most local tools for the users listed in `mx_dtf_ssh_bypass_user`, or set to *False* to always use SSH tools that execute locally. The default setting is set to *True*.

Audit Log

HP Systems Insight Manager (HP SIM) logs all tasks performed by all HP SIM users on all systems. The information is stored in the Audit Log file on the central management server (CMS). Several features of the HP SIM Audit Log are configurable. For example, you can specify which tools log data and the maximum Audit Log file size. The HP SIM Audit Log is configured through the `log.properties` file and tool logging, is enabled or disabled through the XML tool definition files.

Configuring the HP SIM Audit Log

Configuring the HP SIM Audit log is performed from the command line interface (CLI), and you must be signed in as root or administrator.

Configuring the Tool Definition Files

The XML tool definition file provides an option to disable logging of single-system aware (SSA) and multiple-system aware (MSA) command tools. The `log` attribute for the command element specifies whether the results of the command are output to the HP SIM log file. Command output is logged by default.

Configuring the `log.properties` File

You might need to create the file and name it `log.properties` if one does not exist in the directory. HP SIM uses default values when the file does not exist or when a variable is not defined in the file. Refer to “Configuring the Audit Log File” for more information.

Related Topic

- Viewing the Audit Log

Viewing the Audit Log

HP Systems Insight Manager (HP SIM) logs all tasks performed by all HP SIM users on all systems. The information is stored in the Audit Log file on the central management server (CMS).

Note:



You must be signed in as root or administrator (or any user with full-configuration-rights) to read the Audit Log file directly.

To view the HP SIM Audit Log for information recorded in the CMS:

1. Select **Tasks & Logs->View HP SIM Audit Log**. The **Audit Log** page appears.
2. Select the log entries you want to view by selecting one of the following options:
 - **most recent 40 entries**. Select this to view a selectable number of the most recent log entries. The default is set to view the 40 most recent log entries.
 - **from entry " " to entry " "**. Select this option to view an indexed range of log entries.
3. Click **View Now**. The requested log entries appear.

Log Content

The HP SIM Audit Log contains the following information in the order listed, and the log entry key @!@ precedes all other fields in an audit log entry.

- Time stamp date, time, and time zone
- Category
- Result
- Action
- Object type
- Object type descriptor
- Level
- Session user login string
- Session ID (optional)
- Transaction ID (optional)
- Session user full user name (optional)

These fields are displayed in one line. If messages or additional information about a log entry is present, it appears in the next line.

Example of HP SIM Audit Log:

```
@!@,2003-07-11 18:21:50 MDT,CONFIG,SUCCESS,ADD,TASK,Default Automatic  
Discovery,SUMMARY,mxadmin,0,11,
```

```
@!@,2003-07-11 18:22:06 MDT,CONFIG,SUCCESS,MODIFY,TASK,Initial Hardware  
Status Polling,SUMMARY,mxadmin,0,12,
```

```
@!@,2003-07-11 18:51:01  
MDT,CONFIG,SUCCESS,ADD,AUTHORI,MX_AUTH,SUMMARY,jsmith,590,1186800129,
```

John Smith Added authorization for user djones with a toolbox of **Monitor Tools** for All Managed Systems.

@!@,2003-07-11 18:53:08 MDT,CONFIG,SUCCESS,MODIFY,TASK,Hardware Status
Polling for Servers,SUMMARY, mxadmin,0,88,

Related Topic

- Audit Log

Configuring the Audit Log File

Configure the Audit Log file to reside in a user specific directory.

To configure the Audit Log:

1. For Windows, create a file named `path.properties` under `C:\Program Files\HP\System Insight Manager\config`.

For Linux and HP-UX, create a file named `path.properties` under `/etc/opt/mx/config`.

2. Add the following entry in the `path.properties` file: **LOG=\\Auditlog\Logs or LOG=C:/Auditlog/Logs** .

Note: `C:\\Auditlog\Log` is listed here as an example. This path is user defined.

3. For Linux and HP-UX, restart the HP Systems Insight Manager (HP SIM) daemons (**mxstop** and **mxstart**). For Windows, restart the HP SIM service. After restarting the service, a new log file named `mx.log` resides in the directory specified in `path.properties` file.

Five variables can be defined in the `log.properties` file:

- `MX_LOG_FILENAME` for the file name. The default is "`MX_LOG_FILENAME=mx`".
- `MX_LOG_FILEEXT` for the file extension. The default is "`MX_LOG_FILEEXT=log`".
- `MX_LOG_FILESIZE` for the maximum file size. The default is "`MX_LOG_FILESIZE=20`".
- `MX_LOG_ROLLFILEEXT` for the file extension of the roll-over name. The default is "`MX_LOG_ROLLFILEEXT=old`".
- `MX_LOG_QUEUE_SIZE` for the amount of memory allocated for queuing items to be written to the Audit Log. The default is "`MX_LOG_QUEUE_SIZE=300`".

The maximum file size is set in megabytes.

When the Audit Log file reaches the maximum file size, the log is renamed with `MX_LOGROLLFILEEXT` extension, and a new file is started. If a previous version of the file has already been renamed with the `MX_LOG_ROLLFILEEXT` extension, it is an automatic roll-over of an audit log file. A roll-over occurs after a task running is completed. However, after one hour exceeding the maximum file size, if the task is not finished, the audit log file rolls over to another file.

Caution:



Change the queue size only with extreme care. If the queue is set too high, the log manager consumes too much system memory.

Changes made to the `log.properties` file do not take effect until the log manager daemon is restarted. For Windows, restart HP SIM service. For Linux and HP-UX, restart the log manager.

Note:



By default, for Linux and HP-UX, the path for the log file is set to `/var/opt/mx/logs`. This path can be configured by editing the `LOG` value in the `/etc/opt/mx/config/path.properties` file. If this properties file does not exist, create it. For Windows, the default location is the `logs` subdirectory of the directory where the product was installed.

Related Topics

- Audit Log
- Viewing the Audit Log

Troubleshooting

Authentication	Automatic Event Handling	Browser
CIMOM	CLI	Cluster
Collection	Custom Command	Database
Discovery	Event/SNMP Trap	Firmware Upgrade
Generic	HP SIM	HTTP Event
Identification	Integrated Lights-Out (iLO)	Internet Explorer
Installation	IP Address	OpenSSH
Operating System	Paging Notification	Ping
Printing	Property Pages	Protocol
Replicate Agent Settings	Response	Search
Security	Serviceguard Manager	Sign In
SNMP Agent	Software Status	Storage System
Switch	System	System Page
Task	Tools	VCRM
VMM	Virtual Machine	Windows NT Event Log
WMI Mapper		

Authentication

HP Systems Insight Manager (HP SIM) was running fine, but now I receive error messages in the console, such as authentication failure and error accessing database, when trying to run HP SIM.

Solution: To resolve this issue, be sure that the DNS server correctly associates the network address used by HP SIM with the host name of the CMS. If you are using a DHCP server to assign the central management server (CMS) IP address, statically allocate the IP address. You cannot change the host name of the HP SIM.

Automatic Event Handling

Some of my Automatic Event Handling messages appear garbled.

Solution: If you are running an old version of the Microsoft Exchange Server (for example, 5.5) and have problems opening an HTML e-mail message sent from the HP SIM event handler, then the Microsoft Exchange Server must be updated to support the CP1252 character set and map CP1252 to US-ASCII. See <http://support.microsoft.com/default.aspx?scid=kb;en-us;184772> for more information.

Browser

When I try to browse to the System Management Homepage on the same Linux system on which HP SIM is installed, I receive multiple browser warning messages.

Solution:

1. Open a terminal window.
2. At the command prompt, enter:

```
cp /etc/opt/hp/sslshare/* /opt/hp/sslshare
```

3. Press the Enter key.
4. At the command prompt, enter:

```
service hpsmhd restart
```

5. Press the Enter key.

When browsing into a Linux or HP-UX CMS on which the HP Insight Management Agents are installed, a Security Alert dialog box appears when I click an Insight Management Agent.

Solution: The Management HTTP server certificate has not been overwritten with the HP SIM certificate because OpenSSL is not configured correctly. On Linux, OpenSSL should be installed in the `/usr/bin/` directory. On HP-UX, OpenSSL should be installed in the `/opt/apache/ssl/bin/` directory. Install OpenSSL to the correct directory, and then create a new HP SIM certificate to resolve this issue.

I am receiving security alert dialog boxes on the System Page when I click a system link to the Insight Management Agents that reside on the HP SIM Server that I am logged into.

Solution 1: If the security alert states that the name on the certificate does not match the name of the site, you can change settings in HP SIM so that links to systems use the same format as the names in the system certificate.

1. Select **Options->Security->System Link Configuration**. The **Systems Link Configuration** page appears.
2. Select one of the available options. View the system's certificate to see the name format it is using.
3. Click **OK**.

If your system certificates use a name format that does not resolve correctly on your network, then select a link format that does. In this case, you continue to see this name mismatch alert even if you have imported the system certificate into the browser trusted list. This condition can be avoided by disabling the check in Internet Explorer. To do this, select **Tools->Internet Options**, and select the **Advanced** tab. Under **Security** settings, deselect **Warn about invalid site certificates**. However, HP **does not** recommend using this procedure, and it should be considered carefully in accordance with your own security policies and guidelines.

Disabling the **Warn about invalid site certificates** setting in your browser reduces your ability to properly identify the HP SIM server or managed system you are browsing to and any external or internal internet sites having nothing to do with Web-based management products.

Solution 2: If the security alert is for another reason, such as an untrusted or invalid certificate, refer to "Browser" [603] for more information.

When accessing HP SIM after installation is complete, I receive a message stating that the host name in the certificate does not match the URL.

Solution: Create a new certificate after installation with the IP address in the **CN** field. Refer to "Creating a Server Certificate" [admin_cert_server_create.html#CreateServerCert] more information. After the new certificate is created, restart the HP SIM service.

I receive a security alert when accessing a system.

Solution: Be sure that you have the system server certificate imported into your browser and that you browse to the system using the same name as specified in the certificate. For example, having **Browsing to localhost** set in **Internet Options** is most likely the cause for this security alert.

I receive the following error message when browsing to different pages within HP SIM:

This window contains both secure and non-secure items

Solution: Several conditions could cause the browser to display this warning message:

- Improper version of Internet Explorer

There is a known problem in Internet Explorer 6.0 that causes this warning message to be erroneously displayed. Pages within HP SIM that are likely to experience the problem include the **Home** page and the **Task Results** page, though this problem is not limited to those pages.

To resolve this problem with the browser, ensure that you have at least version 5.50.4522.1800 by examining the **Version** string in the browser **About** box.

Note:



Do not rely on the **Update Versions** string provided in the **About** box for Internet Explorer. It does not always correctly indicate the service pack. For example, even if it says SP1 it might not be accurate if the version is 5.50.4134.0600. Instead, ensure you have at least version 5.50.4522.1800.

For more information on the problem with Internet Explorer, refer to Microsoft Knowledge Base article Q269682. For more information on how to determine which browser version you have installed, refer to Microsoft Knowledge Base article Q164539.

- Navigating to a system that does not support SSL

If you navigate to a HP SIM **System Page** for a system that does not support SSL, system links to the system specify the usage of HTTP, a non-secure protocol, rather than HTTPS. This condition would cause the browser to display both secure items from HP SIM and non-secure items from the system, thus prompting the warning.

There might be newer versions of the HP Insight Management Agent for your system that support SSL. If there are not or you want to view the system now, click **Yes** to display the non-secure items, or you will not be able to view the system. All data between the browser and the managed system continues to be encrypted using SSL, and data between the browser and the system is not encrypted using SSL. The sign in applet for older HP Insight Management Agent takes special care to separately encode your sign in credentials so that you can securely sign in, but all other data is not encrypted.

Note:



Selecting **Yes** to the warning message removes the lock icon from the browser because portions of the window are not secure. Additionally, the browser might not provide this warning the next time you navigate to a non-secure system until the browser is restarted.

Note:



Single Login is not supported or attempted on systems that do not support SSL.

- An error page displayed in browser

The browser might be attempting to display an error page, in which case it displays this warning message. For more information, refer to Microsoft Knowledge Base article Q184960.

When browsing to Insight Management Agent on the HP SIM Server itself, multiple security alerts appear while browsing the agent.

Solution: This condition occurs under the following conditions:

- Browsing to Insight Management Agent on the same system as the HP SIM Server. For example, the HP SIM Server is named DAMON, and while browsing to HP SIM, you navigate to the **System Page** for DAMON and select one of the Web-based management links such as **System Management Homepage**.
- Both certificates for the Insight Management Agent and HP SIM are not imported into the browser.

Even though HP SIM and the Insight Management Agent are both running on the same system, they are not the same SSL Web server and do not have the same certificate.

To stop the security alert windows from displaying, import both certificate for HP SIM and the Web-based Management Agent into the browser. Refer to "Importing a Server Certificate" for more information. The information provided there can also be applied to importing the Web-based Management Agent certificate as well.

If the security alert is caused by a name mismatch between the name on the certificate and the name on the address, importing the certificates does not resolve the problem. Instead, browse to HP SIM or the Management Agent using the name in the certificate, or browse to one using the certificate name and the other not using the certificate name. For example, browse to HP SIM using the IP address and to the Management Agent using the system name, or browse to HP SIM using the system name and to the Management Agent using the IP address. Using two different names helps separate the two domains in the browser, preventing confusion with different certificates for the same domain. Refer to remaining security problems for more information.

Starting with HP SIM attempts to synchronize its certificate and private key with the local HTTP server for the Insight Management Agent to alleviate this problem. If synchronization has occurred,

the system should be restarted to ensure both HP SIM and the HTTP server restart with the synchronized certificate. Refer to “Synchronizing Certificates” for more details.

CLI

From the command line, I entered `mxmib -f SHIPPING CFGs not preloaded.txt`, and I received the error `The following is an invalid argument value: CFGs`.

Solution: The command `mxmib` cannot handle spaces. Place the file name in quotes, for example, enter `mxmib -f "SHIPPING CFGs not preloaded.txt"`.

The command `mxagentconfig -a cms_name -p password` fails with

`Unknown hostname: 'cms_name' .`

Solution: For verification purposes, use `nslookup cms_name` to test the network name resolution on the managed system. To correct the problem, set up a network name resolution properly on the managed system by adding CMS information to the managed system `/etc/hosts` file.

The command `mxnode -a system_name` or `mxnode -r system_name` fails with: `Unknown host: 'system_name' System ignored`.

Verification: Use `nslookup system_name` to test the network name resolution on the CMS.

Solution: Set up network name resolution properly on the CMS.

I am receiving a message, `Another user is currently using mxmib, please try again`. How do I resolve this?

Solution: This behavior is expected. Run `mxmib -r` to clear the interlock.

MXMIB enables me to compile a MIB with a different file name, but the same internal module name already exists and is a compiled MIB, which is causing inconsistency in the database.

Solution: The module name and file name must be consistent. If the file names do not match, the files might become corrupt.

If attempting to compile a MIB that already exists in the database, the CLI message states that it is importing even though it is actually updating.

I am a member of an existing HP SIM user group, but when I try to run commands from the CLI, I receive an error message, stating `There was a problem connecting to the HP SIM server`. Be sure that:

1. Your user name has been added to HP SIM. Do this by signing into the HP SIM GUI at least one time.
2. Your username and password, if specified, are correctly spelled.
3. HP SIM is running.
4. You used `--` for any long options and double quotes if your username include s a domain. For example, `<commandname> --user "mydomain\myusername" --pass mypassword`.

I ran the command `mxnodesecurity -r -p protocol -n <non-full-DNS-name>` and received a message that the system was removed. However, the system still exists in the `mxnodesecurity` list.

Solution: To delete a system from the `mxnodesecurity` list using the command `mxnodesecurity -r -p protocol -n <hostname>`, use the fully qualified domain name in place of `<hostname>`.

I am a full-configuration-rights user. However, I receive an exception when trying to run the CLI commands.

Solution for `mxnodesecurity`: On a Linux system, the command must be executed by the root user.

Solution for all CLI commands:

- If you are a member of an HP SIM user group, sign in to the HP SIM GUI at least one time. After that, you will be in the list of authorized users and will be able to run commands from the CLI.
- On a Windows system, you must be a member of the Windows Administrators group to execute CLI commands.

CIMOM

I have a common information model object manager (CIMOM) on a discovered network, but I do not receive any information from the port.

Solution: Try one of the following solutions:

- If the CIMOM is installed and listening on a Secure Sockets Layer (SSL) port other than the default port 5989, the new port number must be specified in the `config/identification/wbemportlist.xml` file. For example:

```
<port id="5991" protocol="https">
  <interopnamespace name="root" />
  <interopnamespace name="interop" />
</port>
```

- Verify that the `interop` namespace for your WBEM provider exists in a port element in the `config/identification/wbemportlist.xml` file. If it does not exist, add it to a port element as an `interopnamespace` element, and restart HP SIM.

Note:



Adding new ports or interop namespaces causes the discovery process to take longer because HP SIM tries all possible combinations of ports, interop namespaces, and user name and password pairs on each IP address in the discovery range.

Cluster

A cluster is not identified as a cluster.

Solution: If a cluster is not defined as a cluster or any of its nodes are not identified correctly, be sure all the Cluster Management Agents are installed (if necessary, reinstall) on every cluster node of that cluster.

After manually adding a system as a cluster, the system type does not change, even if the system is not a cluster.

Solution: If you manually add a system as a cluster, the system type might not change even if the system was not a cluster originally. To reset the system type, delete the system and run discovery.

Clusters or cluster nodes are not identified correctly.

Solution: Clusters or cluster nodes might not be found for the following reasons:

- Starting with SmartStart version 6.30, one of the cluster agents is not installed correctly. The executable is installed on the cluster node, but the Windows registry must be updated.
 1. Access the Windows registry (click **Start>Run** and enter **regedit**.)
 2. Create the following key:

Key:
HKEY_LOCAL_MACHINE, "SOFTWARE\Compaq\CompaqCommonClusterAgent\CurrentVersion"

Value: Pathname, %REG_EXPAND_SZ%, "%SystemRoot%\System32\svrclu.dll"

This update is available starting with SmartStart CD 7.4.
- Be sure the IP ranges in automatic discovery are set to include the cluster and cluster nodes (and not exclude them).
- If the name of the cluster or its node has changed, be sure the DNS servers being used by the cluster and HP SIM both have the new name.
- The cluster node might be down.
- The cluster node has Insight Agents older than version 4.22.
- The Insight Agents are not running on the cluster node.
- The SNMP Agents are not running on the cluster node.
- The network traffic is congesting the network for a significant time.
- SNMP community string might not be matching with that of the HP SIM settings.

Verify the following prerequisites are met:

- The Cluster Management Agents must be running on all the cluster nodes.
- The system must be identified as a server or cluster for cluster identification to run against that system during discovery.

The cluster node is not identified properly by discovery.

Solution: The cluster node name for the DHCP server might be different than its Windows NT name. The remedy is to explicitly place the Windows NT computer names into the `LMHOSTS` file on each cluster node, and then run discovery again. Also, be sure the registry key for the `svrclu.dll` has been created. Refer to the previous issue for information on the registry key.

A cluster or cluster node is not displayed in the Cluster Monitor cluster or node resource settings.

Solution: This issue can result from specific HP Insight Management Agent for those Cluster Monitor Resources that were not running at the time discovery was run. Ensure that the correct agents are running on the clusters and cluster nodes, and then run discovery again.

Cluster Monitor is not displaying properly.

Solution: Ensure that your browser is configured to use **Small Fonts** as the **Font Size**.

The list boxes under Cluster Monitor within Settings are not working properly.

Solution: It takes a few seconds for the down arrows to appear on the list boxes. If there is more than one list box, select an option from the first box, and wait a few seconds to select an option from the second box and each subsequent box. If you make a selection too soon, the list boxes might not work properly.

The cluster nodes are not discovered when the cluster alias is used as the system in manual discovery.

Solution: In manual discovery, add the cluster alias and each node separately to ensure they are entered into the database. Alternatively, include the cluster alias and the node IP addresses in the IP range.

What should I expect when running HP SIM on a cluster?

Solution: HP SIM is not a cluster-aware application. If each node of the cluster has an instance of HP SIM installed, each node has a different certificate with the name of the node, not the name of the cluster, unless you have created your own certificates using a certificate server or other certification authority. When browsing to the cluster, if your browser is configured to **Warn about invalid site certificates**, the browser should display a security alert, warning you the name you have browsed to does not match the name in the certificate. If you have not imported the certificate into the browser or the certificate has not been issued by a trusted certification authority, the security alert also informs you of the untrusted origin of the certificate. Verify the certificate is correct and continue.

During a failover, one node fails and the other node becomes active. Because HP SIM is not cluster-aware, any browsers open to HP SIM must be closed, and you must browse to the cluster again. You might again be presented with another security alert, using the certificate of the other node as previously described. If so, verify the certificate and continue.

Any managed system that establishes a trust relationship with the HP SIM server (for example, for Single Login support, Replicate Agents, Update Software, and so on) should trust all nodes of the cluster because any node could be active and issue the desired command to the system. Refer to “Setting Up Trust Relationships” for more information on setting up trust relationships.

I am having problems identifying clusters.

Solution: If you notice that the cluster name or cluster member name is the IP address of the system and not the host name, download the new HP Insight Management Agent for Windows 2000/Server 2003 for each cluster member of the cluster.

1. Go to <http://www.hp.com>, and click **Support & Drivers**.
2. On the **Support & Drivers** page, under **Or Select a product category**, click **Servers**.
3. Click **ProLiant and Pentium/Xeon servers**.
4. Click **Compaq ProLiant Servers**.
5. Select the appropriate ProLiant series, for example, **Compaq ProSignia 720 server series**.
6. Select the appropriate server, for example, **Compaq ProSignia 720 server 3/350-512**.
7. In the **tasks for your selected products** box, click **download drivers and software**.
8. In the **select operating system** list, select the appropriate operating system ,for example, **Microsoft Widows 2000**.
9. In the **select a category** list, select **Software - System Management**.
10. Click **HP Insight Management Agent for Windows 2000/Server 2003**.

The agents are installed.

Collection

While trying to create a duplicate collection name in a Shared or Private section, an error message is generated.

Solution: Duplicate collection names are not allowed in Shared or Private sections. You can have the same collection in the Shared section as you do in a Private section, but not two collections by the same name in one section.

After deleting a system, the product name or web agent criteria are not removed.

Solution: After a product name or Web agent is discovered, that search criteria remains in the database until the database is reinstalled, which enables you to search on criteria that was present once and might be present again in the future (for example, base tasks on a collection with these criteria, and set it to run when new systems or events meet the search criteria).

Machine names that have spaces within their name are truncated at the space character in a collection.

Solution: When HP SIM writes a discovered system to the SQL database, SQL truncates the name if a space occurs in the machine name. Rename the system without a space.

When trying to sort a collection, it sometimes requires multiple clicks for the column to sort.

Solution: Quick mouse movements inhibit the applet from reading mouse clicks. Hold the mouse absolutely still while clicking the column to sort.

When sorting a search by IP address, the addresses are not listed in numerical order.

Solution: The IP addresses are listed in numerical order, which implies an order like 122.22.22.15, 122.22.22.152, 122.22.22.155, 122.22.22.17, 122.22.22.171, 122.22.22.18. HP is investigating the possibility of providing a fix in a later release

Custom Command

My custom command fails with the following error:

```
C:\Program Files\OpenSSH\bin\switch.exe: *** ca t create title mutex
'Global\cy gwin1S3-2003-11-04 16:46.title_mutex.0', Win32 error 0
```

Solution: The user who is trying to run the custom command is not in the Administrators group. Add the user to the Administrators group.

I cannot find custom commands that I have created.

Solution: New custom tools are added to the **All Tools** toolbox. You might not have authorization to use that toolbox. To view the tool under **Tools->Custom Commands**, add the tool to your authorized toolbox which is present under **Command Line Tools**. Refer to "Editing Toolboxes" for more information.

Database

When trying to reinstall HP SIM on a Windows system from which I previously uninstalled HP SIM, I receive Unable to Create Database. I receive this error during the database creation process.

Solution: This problem is a result of not deleting or renaming the HP SIM database files from MSDE or Microsoft SQL Server after uninstalling HP SIM. Manually delete or rename the database files, and then run the HP SIM installation again.

Discovery

A system that has had a new IP address assigned to it is discovered as a new system in HP SIM instead of having the existing system in HP SIM updated with the new IP address. The original system shows a Critical status.

Solution: This issue results when DNS is not configured on the network. HP SIM tries to use system names from DNS to match previously discovered systems with new systems of the same name. Be sure that DNS is configured on the HP SIM server, and ensure that the DNS server itself is properly configured for the systems in question. Both forward DNS lookups and reverse lookups must resolve to the same system. On Windows, `nslookup <address or name>` can be used to help diagnose the problem.

There is a mismatch between the system table view and the picture view.

Solution: Delete all the systems that are in the affected rack, which includes all the servers, iLOs, enclosures, and switches in that rack, and run discovery on those deleted systems.

Note:



Before deleting the servers, iLOs, and switches, note the IP addresses of these systems, then delete the systems, and run discovery.

After upgrading from HP SIM 4.1 to HP SIM 4.2, my ProLiant BL40p server blade to enclosure associations are displayed as "server in iLO" instead of "server in Enclosure."

Solution: Delete the affected server blades from the database and run discovery again. The server blade to enclosure association will now be displayed correctly.

After running discovery, I noticed that a system was discovered but not identified as a WMI/WBEM device. Why wasn't this system discovered properly?

Solution: A system might not be discovered properly for several possible reasons, including:

- The user credentials were incorrect.
- The provider encounters a problem responding to the WBEM requests.
- The system names can only contain alphabet (A-Z), digits (0-9), minus sign (-), and period (.). However, the system name cannot start with a digit, and the last character must not be a minus sign (-) or period (.).
- On HP-UX or Linux CMS's, no WMIMapper was specified. Therefore, no Windows systems can be identified as WBEM enabled systems.
- There is no provider installed on the target HP-UX or Linux system.

I am trying to delete an HP-UX system, but I receive an error message stating that I cannot delete an HP-UX system that includes a management processor.

Solution: Currently, HP Systems Insight Manager cannot make an association of management processor to server if the system is based on PA-RISC.

Event/SNMP Trap

Why am I not receiving notification when there is a SNMP Authentication trap received?

Solution: The default setting for Enabling Trap Handling in SNMP Extensions is Disabled (Not Processed) because typically, a system can be set up with an incorrect community string or an incorrect community string is set in HP SIM. This error results in an Authentication Failure trap to be sent to the management server each time a request is made to the system, which results in many traps being logged. To change this setting to Processed (Enabled), complete the following steps:

1. Open HP SIM (<http://machinename:280>).
2. Sign in as a user with full-configuration-rights.
3. Select **Options->Events->SNMP Trap Settings**.

4. In the **Mib Name** field, select **rfc1215.mib**.
5. In the **Trap Name** field, select **authenticationFailure** if it is not already selected.
6. In the **Enable Trap Handling** field, select **Yes**.
7. Click **OK**.

These steps set the **Authentication Failure Trap** to be processed, and you are notified of all failures.

After creating a trap forwarding task, specifying several destination servers, and then running the task, only one destination server receives all of the traps.

Solution: Verify that the server sending the traps is also discovered in HP Systems Insight Manager. If it is not, discover the system and then run the task again. All destination servers should receive traps. This problem can happen on a Windows, HP-UX, or Linux server.

Firmware Upgrade

When upgrading my switch firmware, I receive the following error in the log file when I click the succeeded link in the Task Results page:

```
Processed command line: /v 1.1.1 /s /l c:\hpsim_switchfw_logs\
587_11a.wbem.com.log /c /i 170.50.2.3 /f /a swfwupgrade.ini
```

```
Usage: swfwupdate [/c SNMPcommunityString
[/i IPAddr [- IPAddr] ... ]]
[/v FWversion | /b BootVersion] [/m 1 | 2]
[/t TFTPport] [/d] [/l logfile]
[/x IPAddr [IPAddr...]] [/s[ilent]] [/f[orce]]
The /s option requires that /i, /c, and /v also
be specified and implies /f.
The /s option deletes all database entries
prior to discovery.
```

Solution: Verify that the SNMP write community string is set properly for the switch on the **Global Protocol Settings** page.

Generic

The keyboard does not always respond the way I expect.

Solution: If you are used to the Windows operating system, you anticipate the behavior of certain keys, such as the **Tab**, **Enter**, or **Alt** keys. However, in Java applets and Web applications in general, the Windows style is not necessarily used. Therefore, you might need to use the mouse to return focus to a specific page. For example, if you enter an invalid entry for a system IP address or time, the Criteria or Schedule page is refocused, but the keyboard access might not be restored

on the last entry field. This situation typically happens after several attempts. To return the focus, use the mouse to click the page you want to use.

User names are not listed in alphabetical order.

Solution: User names are grouped by authorization level (full-configuration-rights, limited-configuration-rights, and none). Within the groupings, the users are listed in the order they were created.

HP SIM

I receive a message regarding memory address violation when I close the browser.

Solution: You might need to reinstall the SNMP Agent after installing Windows NT 4.0 SP3. If you install Windows NT 4.0 SP4, you must install the SNMP hot fix. The SNMP service has a memory leak and consumes your system resources if you do not install the SNMP hot fix.

After creating a user with full-configuration-rights, the user name is shown in the user list generated from the SQL Analyzer. However, after editing the UserID file, exiting HP SIM, and restarting HP SIM, the user is not listed when selecting Options->Security->Users and Authorizations->Users, although the user name is listed in the database.

Solution: Any attempt to manually modify the UserID file or any user information hash file causes the user account to be removed from HP SIM. Therefore, the user can no longer access HP SIM.

Database connection is lost while using the MIB installer tool, command line MIB Manager, or command line System Type Manager, but the tools indicate successful completion.

Solution: If you lose accessibility to the database when running these command line tools outside HP SIM, you can potentially corrupt the operation you were performing, and predictable results and recovery are not guaranteed.

The Home and Sign Out links are missing in the banner area.

Solution: Click the **Refresh** button at the top of the browser window.

I receive JavaScript errors when the banner attempts to refresh.

I am receiving an HTTP 404 error when launching the Partition Manager through HP SIM.

Solution: If you have reconfigured the secure port for HP SIM, the port must be modified in the `/var/opt/mx/tools/parmgr-web-tools.xml` file. To do this:

1. Edit `/var/opt/mx/tools/parmgr-web-tools.xml`.
2. Modify the port from 50000 to whatever you have configured the secure port to be.
3. Run `/opt/bin/mxtool -m -f /var/opt/mx/tools/parmgr-web-tools.xml` from the command line.

The HP SIM service fails to start on a Windows-based operating system. Failures are shown in the NT application log but do not state an explicit error.

Solution: Search the root directory for a folder or file named `Program`. If this file exists, delete it. If this folder exists, rename it or delete it if the folder is empty.

After signing into HP SIM, no systems, events, or tools are displayed in the console. In some cases, HP SIM might not start correctly or display the Sign In page.

Solution: To resolve this issue, run the database integrity check command (`mxconfigrepo`) from the CLI to verify that dependent items in HP SIM are properly defined in the database.

mxconfigrepo -c

If errors are reported after running this command:

1. Stop the HP SIM service.
2. From the CLI, run **mxconfigrepo -f**.

Caution: If the HP SIM dependent items are not properly defined, running this command (**mxconfigrepo -f**) deletes errant records, which can cause minimal data loss.

3. Start the HP SIM service.

If no errors or reported, call the HP support center.

HP SIM will not start.

Solution: Set the **SNMP Trap Service** to **Manual** instead of **Disabled**.

1. In Windows, select **Start->Control Panel->Administrative Tools->Services->SNMP Trap Services**.
2. Under the **General** tab, change **Startup type** to **Manual**.
3. Click **OK**.

HTTP Event

After creating a new HTTP category, it is not listed in the criteria box on the Advanced Search page when searching for new event types.

Solution: To search for new event types generated by HTTP events, select events by Event Category, and then select the event type from the **and type is** list.

Identification

After running discovery and Identification, the serial number is missing for ProLiant BL p-Class and e-Class switches on the System Page->Identity tab and in the Data Collection report.

Solution: To obtain the serial number for these switches requires support in the firmware of the switches. At this time, this firmware is not available. However, this support is being planned in future versions of the ProLiant BL p-Class switches. There currently is no firmware upgrades being planned for existing switches.

Integrated Lights-Out (iLO)

How do I associate an iLO with a server?

Solution: To associate an iLO with a server, **The Level of Data Returned** must be set to **Enabled** on the iLO itself. Refer to “System License Information Reporting” for more information.

Internet Explorer

Hot keys or other keys, such as Tab and Enter, might not work as expected in the browser.

Solution: Use the mouse to ensure expected results.

During the installation, the system reboots, and then the installation launches the browser. Internet Explorer displays a message saying that it could not establish a connection with the local host. The browser is being launched before the service has had time to start.

Solution: Try to access the URL again by placing the cursor in the URL field and pressing the Enter key. Keep trying until the application loads in the browser.

Sometimes the browser Back button does not take me back to a previous window.

Solution: In Internet Explorer, when the framesets are changed, the browser history is lost. Navigate back through the HP SIM header that is present at all times.

Clicking the browser Back button while viewing a collection returns me to the appropriate system or event overview page.

Solution: This functionality is correct. The browser history is not being updated because of frameset updates. Click the system or event collection to navigate back to the table view page.

I cannot drill down on a collection or an agent link on the System Page.

Solution: When two browsers are open on the same system and they are each pointed to a different HP SIM Management server, unexpected results can occur. Some inconsistencies include not being able to open a collection or not being able to drill down on an agent (for example, Configuration History Reports (Survey Utility)).

I cannot access HP SIM on the local system at `http://localhost:280/`.

Solution 1: Verify proxy server configuration in Internet Explorer. An invalid proxy server address prevents Internet Explorer from browsing to any addresses, including the local system.

Solution 2: Some systems might not be able to resolve the name `localhost`. If this is the case, use `http://127.0.0.1:280/` or `http://machine_name:280`, where `machine_name` is the system on which HP SIM is installed.

When the All Systems window sits idle for an extended period and I launch a new browser window, the All Systems window turns white and Internet Explorer hangs. I am forced to end the task. How can I avoid hanging up in Internet Explorer?

Solution: Avoid leaving Internet Explorer open for extended periods with the **All Systems** collection displayed. Sign out of HP SIM before leaving your monitor to prevent this situation and for security reasons.

I am experiencing unexpected or odd behavior while browsing HP SIM using Internet Explorer.

Solution: This behavior can be caused by a third-party browser extension. Disable these extensions to verify that it alleviates the problem. In the Internet Explorer menu, select **Tools->Internet Options->Advanced**, disable **Enable third-party browser extensions**, and restart all running copies of Internet Explorer.

Installation

I cannot load HP SIM on Windows NT 3.51 or Windows NT 4.0.

Solution: Windows NT 3.51 and Windows NT 4.0 are not supported platforms.

I receive the error Database Connection Error during the Java-based database installation portion of HP SIM installation.

Solution: Verify that the target Microsoft SQL Server service (MSSQL) is running (select **Control Panel->Services->MSSQLSERVER**).

Global Unique Identifiers are the same for all systems when using Disk Imaging software on servers.

Solution 1: If the disk image has not been taken, perform the following:

1. Uninstall all Insight Management Agents from one of the systems.
2. Use the Disk Imaging software to copy the configuration from the system without the Insight Management Agent installed.
3. Use the disk image from step 2 to copy to the target systems.
4. Reinstall the HP Insight Management Agents on all the systems.

Solution 2: If the disk image has already been deployed, perform the following to remove the image from each target system. The following information is divided by network operating systems.

- In NetWare:

The Globally Unique Identifier information is stored in a 16-byte file on the `sys:\system` subdirectory of the NetWare server. This file is created and populated with the Globally Unique Identifier when HP SIM performs an SNMP **SET** command to the NetWare server.

To remove the permanence of the Globally Unique Identifier, delete the file `\system\cpqjbssa.cfg` in the NetWare SYS volume.

After the file is deleted, restart the Insight Management Agent and a new Globally Unique Identifier is assigned by HP SIM when the system is discovered.

- In Windows NT:

The Management Agents create the Globally Unique Identifier information in an entry in the Windows NT registry.

To remove permanence of the Globally Unique Identifier, remove the entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Compaq Insight Agent\hostGUID
```

After the entry is removed, restart the Insight Management Agent services. A new Globally Unique Identifier is automatically generated.

- In UnixWare:

The Globally Unique Identifier information is stored in a file that is created and populated with the Globally Unique Identifier when HP SIM performs an SNMP **SET** command to the UnixWare server.

To remove the permanence of the Globally Unique Identifier, delete the following file from the UnixWare system.

```
/var/spool/Compaq/foundation/registry/cpqhoguid.dat
```

After this file has been deleted, restart the Management Agents. A new Globally Unique Identifier is assigned by HP SIM when the system is discovered.

When installing HP SIM on a Linux or HP-UX system with long host names, the installation fails.

Solution: HP SIM 4.2 supports discovery and management of systems with long host names on Linux and HP-UX (up to 256 characters) but does not yet support being installed on systems with long host names.

On a Windows XP SP2 machine, I receive an error message and the installation does not complete.

Solution: If Simple File Sharing is enabled, it must be disabled.

1. Go to **Start->My Computer->Tools->Folder Options->View**.
2. Scroll to the bottom of the list of advanced settings, and deselect **Use Simple File Sharing (Recommended)**.
3. Click **OK**.

On an HP-UX system, the `mxinitconfig -a` command fails at step 8, and the following error appears in the `/var/opt/mx/logs/initconfig.logfile: ...8. Database Configuration Connecting to database...- Failed HP Systems Insight Manager shutting down: Lost connection to database. org.postgresql.util.PSQLException: Connection refused. Check that the host name and port are correct and that the postmaster is accepting TCP/IP connections. for db loaded from database.props`

Solution: Try the following solutions:

- Ensure that the `semnmi` and `semnms` kernel parameters are set to the minimum values (1024 for `semnmi` and 2048 for `semnms`.)

- The subdirectory `/var/opt/iexpress/postgresql` exists because the PostgreSQL product is not installed or was installed and uninstalled incorrectly. Uninstall PostgreSQL if it is installed, delete the `/var/opt/iexpress/postgresql` directory, and then reinstall PostgreSQL.

IP Address

When systems change IP addresses on the network, the information in the database becomes unreliable. For example, the system name comes from one system, and the description comes from the new system that took that address.

Solution: After systems have been discovered, they can never be "un-discovered." Systems that are no longer reachable must be deleted through a collection (signed in with full-configuration-rights). Systems that HP SIM can no longer communicate with change to Critical status. Systems can be deleted by selecting systems in the collection and clicking **Delete**.

OpenSSH

After installing OpenSSH on a managed system, I cannot find the `.ssh` directory.

Solution: The `.ssh` directory is not created by the SSH installer. Run `mxagentconfig` on the CMS, and enter the target system name (such as, `hpsystem`) and credentials.

I am receiving errors when running OpenSSH, such as `%1 is not a valid Win32 application`.

Solution: Search the root directory for a folder or file named `Program`. If this file exists, delete it. If this folder exists, rename it or delete it if the folder is empty.

Operating System

When the operating system changes on a system and system discovery restarts, HP SIM still discovers an instance of the system running the old operating system with no items in the system links section. HP SIM also discovers the system with the new operating system and with the correct system links.

Solution: After systems have been discovered, they can never be "un-discovered." Systems that are no longer active (the management server can communicate with the system) change to Critical status and can be deleted.

My Evo Workstation 6000 system does not show the correct operating system when it is running Windows XP.

Solution: The root problem is that the SNMP Agent does not correctly recognize this version of Windows. Stop the SNMP service, set it to a manual startup, and run Data Collection from HP SIM again to get the correct information.

Paging Notification

On an upgraded version of HP SIM, which has a paging user upgrade, I am receiving an error, indicating that the user does not exist!, but I can see the user on the Users page. Why do I get this message?

Solution: A user with full-configuration-rights must delete the existing paging user and create a new paging user with the same details as the original paging user.

To resolve:

1. Select **Options->Security->Users and Authorizations->Users**.
2. Find the paging user in the Pager Configured column. **Yes** appears if the user is a paging user.
3. Select the user account to delete.
4. Click **New**.
5. Create a new paging user account.
6. Click **OK**.

Ping

I am not able to ping discovered systems.

Solution: If you manage more than 1,000 systems in HP SIM, tune the kernel parameters by adding the following entries to the `/etc/sysctl.conf` file:

```
net.ipv4.neigh.default.gc_thresh3 = 4096
```

```
net.ipv6.neigh.default.gc_thresh3 = 4096
```

After adding the entries, reboot the system.

Printing

When printing a container view page that includes a Rack Display, the display does not print correctly.

Solution: In Internet Explorer, select **Tools->Internet Options**, then select the **Advanced** tab. Select **Printing->Print background colors and images**. The system Details page should now print the Rack Display correctly, showing all details of the rack.

When trying to print in Internet Explorer, I am receiving a message, stating that my printer is not configured. In Mozilla, the print dialog box appears to print to a file.

Solution: The printer must be installed before trying to print in both Internet Explorer and Mozilla.

When printing lists or reports in HP SIM, selecting Landscape as the paper orientation is not changing the printout to landscape.

Solution: From **Control Panel->Printers**, set the orientation to **Landscape**.

Property Pages

I receive the following error message on the Property pages:

Error: Cannot connect to target system using WBEM. Check WBEM protocol settings for this system under Options->Protocol Settings->Global Protocol Settings.

Solution: The target system has been identified as WBEM enabled, but the credentials are failing for the target system. Verify the credentials, and identify the target system again.

I receive the following error message on the Property pages:

Unknown WBEM error.

Solution: An unanticipated WBEM error has occurred. Contact HP Support.

I receive the following error message on the Property pages:

Communication has been lost. Close the window and relaunch Properties for this system.

Solution: The **Property** pages are subject to the Web server default tim-out (20 minutes). If the **Property** pages time out, this message appears. Close the window, and relaunch the **Property** pages against the target system.

I receive the following error message on the Property pages:

Property pages are unavailable because this system acts as a WBEM storage proxy.

Solution: The target system contains a WBEM installation (CIMOM) that is a storage proxy CIMOM. There is not a WBEM CIMOM that models the target system. Therefore, the **Property** pages do not have an agent that collects system-specific information. Install a server WBEM CIMOM to enable WBEM manageability for the target system.

Protocol

When adding a client to the CMS, the WBEM protocol is not displayed under management protocols, and none of the WBEM properties are listed on the System Page for the client.

Solution: The password might be incorrect on the **System Protocol Settings** page (Options->Protocol Settings->Global Protocol Settings).

I receive the error message <<<CANNOT BE BLANK, and the Schedule and Run Now buttons are disabled.

Solution: If a field is left blank on the **System Protocol Settings** page, this message appears. Fill in the blank fields, and the buttons will be enabled.

Replicate Agent Settings

When running a Replicate Agent Settings task with the Wake target systems from low power mode before configuring option selected, I receive the following error on the Task Results page in the Task Details section: Failed to power up system.

Solution:

1. Release and renew the IP address of the system.
 - a. In Internet Explorer, click **Start->Settings->Network and Dial-up Connections**.
 - b. Double-click **Local Area Connection Status**. The **Local Area Connection Status** window appears.
 - c. Click **Properties**. The **Local Area Connection Properties** window appears.
 - d. Select **Internet Protocol (TCP/IP)**, and click **Properties**. The **Internet Protocol (TCP/IP) Properties** window appears.
 - e. Update the IP address accordingly.
2. Delete the system from the database, and rediscover the system. Refer to "Configuring Automatic Discovery" for more information on running discovery.
3. Run the Replicate Agents Settings task. Refer to "Creating a Replicate Agent Settings Task" for more information.

When running a Replicate Agent Settings task, I receive the following error on the Task Results page in the Task Details section: No is not true: Wrong compaq.cimom.supported.

Solution: This message indicates that the system does not have any Web Agent that supports being configured by way of Replicate Agent Settings. It is possible that the Replicate Agent Settings, such as System Management Homepage, were not running during discovery or were not installed on the target system. Verify that there is a System Management Homepage link on the system page in HP SIM. If there is no System Management Homepage link, try to deploy one by using the Initial ProLiant Support Pack installation.

Response

It takes five minutes or more to load when https:// is entered in the URL address.

Solution: The URL address should be entered http://, without the "s." When https:// is entered in the URL, an SSL message is sent to the server, causing delay.

When browsing to the Web Agents or to System Management Homepage on a remote system from HP SIM, the browser displays Page Note Found.

Solution: There are several possible solutions:

- It might be that the Web Agents or the System Management Homepage is no longer running on the remote system. They must be started to be accessible.
- It might be that the remote system is not reachable from your browser. If the HP SIM server is managing systems on two networks and your browser client is only on one network and the remote system is on the other network, then it will be unreachable.
- It might be that the address of the target system is not correctly resolving to the proper IP address. There might be a problem in the DNS configuration of your network. If so, and it is beyond your realm of control, you can alleviate the problem by adding the remote system name and its real IP address to the hosts file on the HP SIM server, the browser system, or both. Another

solution is to modify the **Options->Security->System Link Configuration** settings in HP SIM, and select **Use the system IP address**.

Search

When searching for systems on which the operating system is the single version of HP-UX 11.11, two criteria are displayed in the operating system collection. If I select HP/HP-UX 11.11, the CMS appears. If I select HP-UX/HP-UX B.11.11 U, all of the HP-UX systems are displayed except the CMS.

Solution: Instead of selecting **is** in the comparison selection box, select **contains**, and then enter **HP-UX 11.11**.

Security

Executing a tool on a managed system results in the error: Authentication failure: The central management server (CMS) and managed system time clocks might not be synchronized, or a communication time limit might have been exceeded.

Solution: The CMS and managed systems must be time-synchronized to prevent authentication failures. The communication time limit is 20 minutes, and exceeding this limit causes authentication failures. Use the command **xntpd (1m)** to configure the time synchronization.

I am unable to Single Login or set the trust status to Linux agents.

Solution: To resolve this issue, configure the System Link Configuration setting to IP address or full DNS name.

To configure the System Link Configuration setting:

1. From the HP SIM CMS, select **Options->Security->System Link Configuration**. The System Link Configuration page appears.
2. Select one of the following options:
 - **Use the system IP address** to specify IP address
 - **Use the system's full DNS name** to specify full DNS name
3. Click **OK**. Your setting is saved.

Serviceguard Manager

When upgrading from SCM 3.0 with Serviceguard Manager installed to HP SIM 4.1, Serviceguard Manager no longer runs.

Solution: When HP SIM is upgraded, some of the files that Serviceguard Manager installs are replaced so that it appears that Serviceguard Manager is not installed. Reinstall Serviceguard Manager.

When I launch Serviceguard Manager, I am asked to download a `.jnlp` file. The following scenarios might appear when installing Serviceguard Manager.

Scenario 1: Java Web start not installed.

Solution: Download and Install Java Web start.

Scenario 2: Java Web start is installed, but you are still being asked to download the `.jnlp` file. Refer to one of the operating systems in the following list for the solution.

Windows 2003 IE Browser Solution:

1. Download the `.jnlp` file.
2. Right-click the `.jnlp` file.
3. Select **Open with...and Choose Program**.
4. Click **Browse**.
5. Navigate to and open `C:\Program Files\Java Web Start\javaws.exe`.
6. Select **Always use this program to open these files**.
7. Click **OK**.

Linux Mozilla Browser Solution:

1. Click **Launch Serviceguard Manager**.
2. Select **Open with...and Choose Program**.
3. Click **Choose**.
4. Navigate to `/usr/java/j2re1.4.2/javaws/javaws` .
5. Select **Always perform this action**.
6. Click **OK**.

HP-UX Mozilla Browser Solution::

1. Click **Launch Serviceguard Manager**.
2. Select **Open with...and Choose Program**.
3. Click **Choose**.
4. Navigate to `/opt/java1.4/jre/javaws/javaws`.

Note:



If this path is not present, install the T1456AA with Java Web start.

5. Select **Always perform this action**.
6. Click **OK**.

I received an HTTP 404 error when I tried to launch Serviceguard Manager.

Solution: After installing HP SIM, Serviceguard Manager must be installed on the CMS platform (Windows, Linux, HP-UX). At this time, SGM is registered with HP SIM. If, at a later time, you uninstall Serviceguard Manager, you will receive an HTTP 404 error if you try to launch it. Because the Serviceguard Manager uninstall application deletes the directory `sgmgr` under the HP SIM webapps directory, which is located at `/opt/hpwebadmin/webapps` on HP-UX and Linux and at `\Program Files\HP\System Insight Manager\hpwebadmin\webapps` on Windows.

To avoid the HTTP 404 error in the future, remove the tool from HP SIM using the following command:

```
mxtool -r -f sgmw-web-tools.xml
```

If Serviceguard Manager is reinstalled in the future, add the tool to HP SIM again, using the following command:

```
mxtool -a -f sgmw-web-tools.xml
```

Sign In

I cannot sign in to HP SIM on Windows XP using a blank password.

Solution 1: Use a non-blank password, which provides better security. Have an administrator reconfigure the Windows User Accounts to specify a non-blank password.

Solution 2: If you must use a blank password, disable the following **Security Policy** on the Windows XP machine: **Accounts: Limit local account use of blank passwords to console login only**.

Note:



Disabling this policy allows remote logins over the network using accounts that have no passwords.

On a Windows system, to limit local account use of blank passwords to console sign in only, complete the following procedure:

1. Open Local Security Settings MMC Application by selecting **Programs->Administrative Tools->Local Security Policy**.
2. Open the **Local Security Policies** folder, and then open the **Security Options** subfolder.
3. Disable the policy.

I cannot to sign in to HP SIM on Windows XP.

Solution: If using a blank password, refer to the preceding problem. Otherwise, change the following Local Security Policy on the Windows XP machine: **Network Access: Sharing and security model for local accounts** from Guest Only to Classic.

Note:



This setting does not affect remote sign ins using domain accounts. Modifying this policy allows remote sign ins over the network using any local account configured to do so, not just the Guest account. Ensure all local accounts have appropriate passwords.

To change the setting:

1. Open Local Security Settings MMC Application by selecting **Programs->Administrative Tools->Local Security Policy**.
2. Open the **Local Security Policies** folder, and then open the **Security Options** subfolder.
3. Change the setting from Guest Only to **Classic**.

If Guest Only is the preferred policy setting, perform the preceding steps, sign in to HP SIM, and then add domain accounts (not local accounts) or the local Guest account as accounts to HP SIM. Restore the local policy setting back to Classic when done.

Single Login fails on cluster systems.

Solution: Single Login does not work on a virtual cluster system. It works on the physical systems that comprise the cluster.

By using a proxy server, you might inadvertently or intentionally bypass IP address login restrictions configured for the user.

Solution: A proxy server can be used to bypass specific IP exclusions, if the proxy server IP address is not included in the IP exclusion ranges on the **Login IP Address Restrictions** page. Likewise, the possibility that a valid proxy server is included in the IP exclusion ranges would prevent a valid user from signing in through that particular proxy server.

Ensure valid proxy servers are within a valid Inclusion ranges, and make the Inclusion ranges as small as possible. Using IP inclusion ranges is more effective than using IP exclusion ranges because Inclusion ranges exclude all addresses not specified in the IP inclusion range.

I cannot sign in to HP SIM or to managed systems browsing from HP SIM using Internet Explorer 6.0.

Reason 1: Internet Explorer has a problem with underscores in system names, which prevents the authentication cookie from working properly.

Solution 1A: For HP SIM, if you are using Internet Explorer 6.0 and your HP SIM server has an underscore in the name, use the IP address of the HP SIM server instead of the name in the Internet Explorer address field.

Solution 1B: For managed systems, if the names of the systems have an underscore, use the IP address of the system. Configure HP SIM to create links to the system using the IP address instead of the name:

1. Browse and sign in to HP SIM.
2. Select **Options->Security->System Link Configuration**. The System Link Configuration page appears
3. Select Use the system IP address.
4. Click **OK**.

Note: By using IP addresses instead of names, you might encounter security alerts, if the name in the managed system certificate does not match the name in the link. The default certificate for managed systems uses the system name, not the IP address.

Reason 2: For managed systems, the privacy policy setting in Internet Explorer 6.0 is blocking the authentication cookies from the managed systems.

Solution 2A: Change the browser privacy security policy setting. From the Internet Explorer browser menu, select **Tools->Internet Options**, and select the **Privacy** tab. The privacy setting can be modified in one of the following ways:

- Set the privacy setting to **Accept all Cookies** by sliding the slider bar to the bottom. This setting allows a browser to accept all cookies for both first-party and third-party sites. When browsing to HP SIM or directly to a managed system, it is considered a first-party site. When navigating to a managed system through HP SIM, the system is considered a third-party site.
- Customize the handling of cookies by clicking **Advanced** and enabling **Override automatic cookie handling**. Then select the appropriate radio buttons for first-party and third-party cookies to **Accept** or **Prompt**. If you select **Prompt**, the browser prompts you on how to handle a cookie each time a cookie is received. You can choose to block or allow the cookie each time or for every time. Enabling **Always allow session cookies** does not resolve the problem because the Web Agents do not use session cookies.
- Individually specify the handling of cookies for each system. Click **Edit** in the **websites** section and add the address of the system in the specified field. Click **Allow** to always allow cookies to that system. Repeat this for all systems.

Solution 2B: Remove the systems from the Internet Zone. The privacy policy only affects systems in the browser Internet Zone, so by removing systems from that zone, you prevent the privacy policy from affecting those systems. This configuration can be accomplished in one of the following ways:

- Browsing to systems by IP address instead of by name can cause the browser to consider those systems to be in the Internet Zone. Instead, browse by name. You can configure HP SIM to use system names when creating links to systems by selecting **Options->Security->System Link Configuration** and selecting **Use the system name**.

- If your browser is configured to use a proxy server, you can configure your browser to bypass the proxy server for specific systems, which removes those systems from the browser **Internet Zone**. From the browser menu, select **Tools->Internet Options**, and select the **Connections** tab. Click **LAN Settings**, and if you are configured to use a proxy server, click **Advanced**. In the **Exceptions** list, you can specify a list of addresses that should bypass the proxy server. These addresses are no longer in the **Internet Zone** and are not affected by the privacy settings policy.

Selecting a link that opens a new browser window requires another sign in.

Solution: If you are browsing using the Internet Explorer link from within Windows Explorer, you must instead start Internet Explorer as a separate process. Start Internet Explorer by selecting it from the Windows Start menu or using the desktop icon.

I cannot sign in to the HP SIM server from Windows NT, Windows 2000, or Windows XP.

Solution: The Windows accounts used to access HP SIM must have the **access this computer from the network** right selected.

In Windows NT 4, open the User Manager by selecting **Start->Programs->Administrative Tools**. In the **Policies** menu, select **User Rights**. In the **Rights** dropdown list, select **access this computer from network**, and ensure the HP SIM users are granted full-configuration-rights.

In Windows 2000 and Windows XP, open the Local Security Policy by selecting **Start->Programs->Administrative Tools**. Expand the Local Policies tree, and select **User Rights Assignment**. Ensure the HP SIM users have the **access this computer from the network** right and that they do not have the **Deny access to this computer from the network** right selected.

I am receiving the exception org.apache.jasper.JasperException while signing in to HP SIM.

Solution: Delete all the files in the `work` directory, and sign in again.

- On HP-UX and Linux: `/opt/mx/jboss/server/hpsim/work`
- On Windows: `\jboss\server\hpsim\work`

I am being asked for my signin credentials when accessing a trusted system.

Solution: Verify that you have a valid trust relationship set up between HP SIM and the managed system. Also, verify that you are authorized for an appropriate tool on the desired system. Tools that enable Single Login to managed systems include System Management Homepage as Administrator, System Management Homepage as Operator, System Management Homepage as User, Replicate Agent Settings, and Install Software and Firmware. Refer to "Setting Up Trust Relationships" for more information on setting up trust relationships.

After installing the Microsoft MS04-025: Cumulative Security Update for Internet Explorer (867801), I can no longer access HP SIM and System Management Homepage.

Solution: This issue affects any system running Windows XP Service Pack 2 and any version of HP SIM and System Management Homepage or any system running Windows XP Service Pack 2 and browsing to HP SIM running on any supported operating system. To resolve:

- Configure Windows XP Service Pack 2 firewall to allow access to System Management Homepage.
 1. On the Windows XP system, select **Start->Control Panel->Windows Firewall** to configure the firewall settings.
 2. Select the **Exceptions** tab, and click **Add Port**.
 3. Add the following exceptions to the firewall protection. Enter the product name and the port number for each.

Description	Port	Protocol
HP SMH Web Server*	2301	HTTP
HP SMH Secure Web Server*	2381	HTTPS
WBEM/WMI Mapper	5988	HTTP
WBEM/WMI Mapper Secure Port	5989	HTTPS
SSH port	22	SSH
SNMP Agent	161	SNMP
Ping Discovery (ICMP)**	***	ICMP
Ping Discovery (TCP)**	80	HTTP

* If the system is not being managed from HP SIM, only ports 2301 and 2381 should be configured to enable browser access to System Management Homepage.

** Usage is configurable in HP SIM.

*** This setting is under the **Advanced** tab of the **Windows Firewall** window. Select **ICMP Setting->allow incoming echo request**.

4. In the **Add a Port** window, click **OK**.
5. In the **Windows Firewall** window, click **OK**.

This configuration leaves the Windows XP Service Pack 2 security enhancements intact and allows traffic over the ports listed in the previous table.

Note: HP SIM discovers Web servers on other ports

- Enable file and print sharing and Remote Administration Exception.
 1. Enable file and print sharing:
 - a. Select **Start->Control Panel**.
 - b. Click **Windows Firewall** to configure the firewall settings.
 - c. Select the **Exceptions** tab.

- d. Select the **File and Print sharing** checkbox.
 - e. Click **OK**.
2. Enable Remote Administration Exception:
 - a. In the **Control Panel**, open the **Group Policy** editor.
 - b. Select **Computer Configuration**.
 - c. Select **Administrative Templates**.
 - d. Select **Network**.
 - e. Select **Network Connections**.
 - f. Select **Windows Firewall**.
 - g. Select **Domain profile**.
 - h. Select **Enable the Windows Firewall: Allow Remote Administration Exception**.
- Configure Windows XP Service Pack 2 to allow access to HP SIM on the system running Windows XP Service Pack 2 and HP SIM.
 1. On the Windows XP system, select **Start->Control Panel->Windows Firewall** to configure the firewall settings.
 2. Select the **Exceptions** tab, and click **Add Port**.
 3. Add the following exceptions to the firewall protection. Enter the product name and the port number for each.

Product	Port	Protocol
SNMP Trap Listener	162	SNMP Trap (UDP)
HP SIM Web Server	280	HTTP
RMI registry	2367	RMI
JBoss RMI/JRMP Invoker**	4444	TCP
JBoss Pooled Invoker**	4445	TCP
JBoss Web Service port**	8083	TCP
HP SIM Secure Web Server	50000	HTTPS
HP SIM SOAP *	50001	HTTPS
HP SIM SOAP with client certificate authentication*	50002	HTTPS

Product	Port	Protocol
HP SIM SOAP*	50003	HTTPS
HP SIM WBEM Event Receiver*	50004	HTTPS/HTTP*
WBEM Events	50005	TCP
PostgreSQL	50006	TCP
JBoss Naming Service RMI port**	50008	TCP
JBoss Naming Service port**	50009	TCP
HP SIM VMM Essentials v 1.1.2.0	50010	TCP
Web services RMI class loader	50013	TCP
JRMP invoker	50014	TCP
Pooled invoker	50015	TCP

* Configurable in HP SIM

** Configurable in the `SIM/jboss/server/hpim/conf/jboss-service.xml` descriptor

4. In the **Add a Port** window, click **OK**.
5. In the **Windows Firewall** window, click **OK**.

This configuration leaves the Windows XP Service Pack 2 security enhancements intact and allows traffic over the ports listed in the table.

After installing HP SIM, I changed the Windows administrator password and can no longer sign in to HP SIM.

Solution: If you have SQL Server installed locally, verify that it is running. If it is not running verify the logon credentials. The service login credentials could have changed. The HP SIM service is registered to run under the credentials used during installation. To resolve this issue:

1. Change the MSSQL service password:
 - a. In Windows, open **Services (Control Panel->Services)**.
 - b. Locate the MSSQL service and select **Properties**.
 - c. Select the **Logon** tab, and change the password.
 - d. Restart the MSSQL service.
2. Change the HP SIM service password:
 - a. In Windows, open **Services (Control Panel->Services)**.
 - b. Locate the HP SIM service, and select **Properties**.

- c. Select the **Logon** tab, and change the password.
 - d. Restart the HP SIM service.
3. If you are using OpenSSH on Windows Server 2000 or 2003, change the OpenSSH Server service password:
 - a. In Windows, open **Services (Control Panel->Services)**.
 - b. Locate the OpenSSH Server service, and select **Properties**.
 - c. Select the **Logon** tab, and change the password.
 - d. Restart the HP SIM service.

Signing in from a dial-up connection takes a long time.

Solution: Your connection depends on many factors that are beyond your control. You might have a slow modem, the server you are connecting to might not be operating at peak efficiency, or you might have a bad phone line.

I cannot sign in to HP SIM.

Solution: This condition can result from any of the following reasons:

- If the **IP Address Restriction** field (on the **New User Group**, **Edit User**, **New User**, or the **Edit User Group** pages) is configured, ensure that it includes all IP addresses of the CMS. If browsing to *localhost* ensure that the loopback address 127.0.0.1 is also included.
- You are not entering the information correctly. Passwords are case-sensitive.
- The account you are entering is not a valid account for HP SIM.
- The account you are entering has been deleted, disabled, or locked out.
- The password for the account must be changed.
- You are attempting to sign in from an IP address that is not valid for the specified account.
- You do not have cookies enabled in your browser or you are using a cookie blocker.

I cannot sign in to my Windows HP SIM.

Solution: If you are attempting to sign in with a Windows user account created on the CMS (as opposed to a domain account) and the CMS host name is longer than 15 characters, then you must enter the first 15 characters of the CMS name in the domain field to sign in. For example, if your Windows CMS is named "SIMwin2003withsp2" and you have a local account "bob," then sign in with username = "bob" and domain = "SIMwin2003withs." Any new local user account created cannot sign in, unless they were created using only the first 15 characters of the system name entered in domain name field and signed in using the same.

SNMP Agent

How do I enable or disable the Restart Agents option that is available for the SNMP Agents when using the HP SIM Replicate Agent Settings Task?

Solution: The option must be changed from inside the HP SIM Replicate Agent Settings Task.

1. Select **Configure** > **Replicate Agent Settings**.
2. Select a target system, and click **Next**. Refer to "Creating a Task" for more information on selecting the target system.

Note:



The source system must have a trust relationship with the HP SIM Server. Refer to "Requiring Trusted Certificates" for more information.

3. Select the **configure** link related to system.
4. On the **Insight Management Agent** page, under the **Restart Agents** option, select the **Enable** or **Disable** radio button.
5. Click **Apply**, and close the **SNMP Configuration** page.
6. Return to HP SIM, and click **Refresh**. The updated configuration appears in the Replicate Agent Settings Task
7. Complete the Replicate Agent Settings Task setup by clicking **Next**, defining a task name, selecting a collection, and defining a schedule for the task. Click **Save** to complete the setup and return to the **Tasks Results** page.

Note:



Restart the agent on the source system after finishing the Replicate Agent Settings Task to cause the changes to take effect.

Software Status

The SW Status column displays Unknown. How do I determine why the status is Unknown?

Solution: There are several reasons why the **SW** Status displays Unknown. To assist in determining why a status is unknown, position the cursor over the **SW** Status column that displays Unknown. A tool tip appears and displays a hint indicating what is unknown. Any of the following can display:

- HP Version Control Repository Manager not found

- Possible VCA trust issue
- Software Status Polling task not run on system

If the status cannot be determined, then the tool tip displays `Click for Details`.

Storage System

Sections of a storage system's Identity tab are missing or say No data available.

Solution: Data has not been collected, or the data collection task was not successful. Try the following solutions:

Note:



HP SIM displays data supplied by a storage system's SMI-S provider. If the SMI-S provider does not supply all of the data that HP SIM can display, the table containing that data will say `No data available`, even though data collection was successful.

-
- Verify that HP SIM is configured to discover and collect data from storage systems. Refer to “Configuring HP Systems Insight Manager with Storage Systems” for more information.
 - Create and run a new data collection task for the affected systems. Refer to “Creating a Data Collection Task” for instructions.
 - Restart the SMI-S provider. Refer to the SMI-S provider's documentation for instructions.

One or more storage systems is missing from the Storage Systems collections in HP SIM.

Solution: There might be a configuration problem with the SMI CIMOM or the SMI-S provider. Perform the following:

- Verify that HP SIM is configured to discover storage systems. Refer to “Configuring HP Systems Insight Manager with Storage Systems” for more information.
- Verify that your SMI-S provider is installed and configured with SSL enabled. Refer to the *HP SIM Installation and User Guide* for more information about obtaining and installing SMI-S providers.
- Verify that the WBEM SSL port is accessible on the network. On the CMS, open a command window, and enter `telnet providerIPAddress 5989`.
 - If the port is accessible, a blank line appears, and no error such as `Connect failed` or `Connection refused` appears. Press **Control-]**, and enter `quit` to disconnect and close Telnet.
 - If the port is unreachable and the SMI-S provider is correctly installed and configured, verify that there is a firewall between the CMS and the system hosting the SMI-S provider. If there is a firewall, configure it to allow traffic through the port the provider is running on (usually 5989).

Switch

After discovering and identifying an HP ProCurve Switch, the switch management page is not displayed when I click the HP ProCurve switch link under the System Page, Link tab.

Solution: Change the **System Link Configuration** settings for the system.

1. Click **Options->Security->System Link Configuration**. The **System Link Configuration** page appears.
2. Select **Use the system full DNS name** to use the full system DNS name instead of the system name.
3. Click **OK** to save and apply the changes.

Return to the **System Page** for the HP ProCurve Switch, and the link will now open correctly.

System

Systems displaying on the system table view page with Critical status do not display IP/IPX address and have no system link.

Solution: HP SIM has assigned this system address to another node. The following scenarios can cause this issue to occur:

- The system is temporarily removed from the network. When it returns, the system returns to a managed state. This situation can happen when a laptop computer is removed from the network for an extended period and its previous address has been reused by DHCP.
- The system could have changed names. However, this change was not discovered by HP SIM. HP SIM continues to look for a system by that name.

My SNMP parameters are not saved when I add a system with a host file. I created a file that did not exist on the network. For example:

```
#$IMXE: Type="Server"

#$IMXE: SNMP_RET=4 SNMP_TIM=10 SNMP_MON=HP SNMP_CON=HP

1.1.1.1 myserver
```

How can I save the SNMP parameters?

Solution: This problem only exists when a system is not online yet. However, HP recommends the following workaround:

```
#$IMXE_DEFAULT: Type = Server SNMP_RET=4 SNMP_TIM=10 SNMP_MON=HP
SNMP_CON=HP

1.1.1.1 myserver
```

When the All Systems window sits idle for a few minutes and I launch a new browser window, the All Systems window turns white and Internet Explorer

hangs. I am forced to end the task. How can I avoid hanging up in Internet Explorer?

Solution: For security reasons, always sign out of HP SIM before closing Internet Explorer. Signing out before closing Internet Explorer resolves this issue.

When I use the command `mxnode -r -f` to delete systems, the container systems (for example, clusters, enclosures, and racks) are not deleted.

Solution: Containers must be deleted individually.

How do I change a credential for a system that is currently using the global defaults?

Solution:

1. Run the `mxnodesecurity` command to change or add the credentials.
2. Run `mxnode` from the CLI to generate an XML file for a particular system and redirect the output to an external file:

```
mxnode -lf nodename >somefilename.xml
```

where *somefilename.xml* is the name of the external file in which the output is directed.

The following is an example of a partial `mxnode` XML file:

```

    <?xml version="1.0" encoding="UTF-8"?>
    <node-list>
    <node name="abc" guid="..." host-name="abc.mycompany.com">
    <hw-attribute name="DeviceType">Workstation</hw-attribute>
    <hw-attribute name="DeviceSubType">HP9000</hw-attribute>
    <hw-attribute name="Model">9000/785</hw-attribute>
    <hw-attribute name="ProcessorFamily">pa-risc</hw-attribute>
    <sw-attribute name="OSName">HPUX</sw-attribute>
    <sw-attribute name="OSVendor">HP</sw-attribute>
    <sw-attribute name="OSRevision">11.00</sw-attribute>
    <sw-attribute name="IPAddress">192.1.2.3</sw-attribute>
    <sw-attribute name="ProtocolSupport">SNMP:1.0</sw-attribute>
    <sw-attribute name="Description">HP-UX phoenix</sw-attribute>
    <sw-attribute name="SystemName">abc.mycompany.com</sw-attribute>
    <sw-attribute name="DefaultProtoSettings">true</sw-attribute>
    <sw-attribute name="DefaultAttributeSettings">true</sw-attribute>
    <sw-attribute name="DefaultSystemName">true</sw-attribute>
    </node>
    </node-list>

```

3. The last three *sw-attribute* elements represent the current *default* settings (true or false).
4. Edit the file and change all three values to false, and save the file.

5. Use the `mxnode` command to modify the same system, using the modified XML file as input:

```
mxnode -m -f somefilename.xml
```

The system should now use the new settings.

System Page

On the System Page, when I click the Management Processor link, I receive an HTTP 1.1 dependency error and there is no status icon for the Management Processor.

Solution: The iLO and proxy server (if being used) must be configured to use HTTP 1.1.

- **To configure Internet Explorer to use HTTP 1.1:**

1. In Internet Explorer, select **Tools->Internet Options->Advanced**.
2. Under **HTTP 1.1 Settings**, select **Use HTTP 1.1**.
3. Click **OK**.

- **To configure Mozilla to use HTTP 1.1:**

1. Select **Edit->Preferences->Advanced->HTTP Networking**.
2. In the **Direct Connection Options**, select **Use HTTP 1.1** and select **Enable Keep-Alive**.
3. Click **OK**.

- **If you are communicating to an iLO through a proxy server:**

1. In Internet Explorer, select **Tools->Internet Options->Advanced**.
2. Under **HTTP 1.1 Settings**, select **Use HTTP 1.1 through proxy connections**.
3. Click **OK**.

Links on the System Page that participate in HTTP communication do not get updated when an agent is stopped.

Solution: When browsing to a particular system that has a Web Agent (`http://machinename:2301`), the first link/GIF on the window (usually Insight Manager Web Agents) is the proxy agent that sends all HTTP commands. If a Web Agent is stopped that is not the proxy agent, then the appropriate HTTP command is not sent to HP SIM, allowing the link to the Web Agent to be updated. To verify that you have the correct links for a system, execute discovery or the Daily Identification Task, which verifies all Web Agents running on a particular system.

When drilling down on links on the System Page, time-outs occur.

Solution: This error often happens when the HP SIM Management server can see multiple subnets. However, the system that the user is browsing from cannot. When drilling down on some links (like Management Agents), HP SIM connects to `http://systemIPaddress:2301` with added URL

information. This link connects directly to the agent running on that system. The machine that the user is browsing from must be able to speak to the system in question through TCP/IP (for example, be able to ping the system).

When drilling down on a Critical system, the System Page still displays all links that were present before HP SIM could not talk to the system.

Solution: This behavior is expected. Links remain in case the system in question is in a reboot state or some other state of flux. If the system is actually down, the links time out when connecting to any agent or Web server.

Task

When creating a task, I cannot use the Backspace key to delete text in any of the text boxes. How can I edit my entry?

Solution: When creating a task, use your mouse to select the text to be corrected, or use the Delete key to delete text from the text box. Enter the updated information.

When executing a task, the message `Unknown OS` appears.

Solution:

1. If the system that you are trying to execute a task against is a Windows system, verify that it was rebooted after installation of SSH. A reboot is required to complete the installation.
2. Enable DMI, WBEM, or SNMP on the system so the type of operating system can be determined, and then run identification and data collection to update the HP SIM database.
3. Verify that the commands to determine the operating system are working.

For Windows. `ver`

For HP-UX and Linux. `uname`

When running the Initial ProLiant Support Pack Install task, it fails.

Solution: When running the Initial ProLiant Support Pack Install task on a Windows 2000 or Windows 2003 system, be sure to enter the domain in the **Domain** field. If the system is not part of the domain, enter the target system name instead.

On an HP-UX system, when a full-configuration-rights user edits a task, changes the owner to a limited-configuration-rights user, and then views the task, the original owner is still shown as the owner. If a full-configuration-rights user opens another browser and views the task, the correct owner appears.

Solution: This is a sporadic error with no known solution.

After executing the Install Software/Firmware task on a Windows 2000 Advanced Server system, the status does not update in the Task Results section. The status continues to report In Progress, and the Install Software/Firmware task finally times out after two hours.

Solution: The Linux VCA target system cannot resolve the address of the CMS. Ensure whether the name resolution is configured properly, and if it is not working, the Linux system that has the VCA installed must be configured to include the CMS name in the host file.

To configure the host file on the Linux system:

1. Edit the host's file in `\etc` directory.

Note: You can use a text editor or `vi` to edit this file.

Add an entry in the host file:

- `<ipaddress of server> <fully qualified DNS name of server> <name of server>`

For example, an HP SIM system with IP address `170.50.1.201`, fully qualified domain name `perf760g2.wbem.com`, and name `perf760g2` displays the following entry in the host file of the managed node on the Linux VCA system:

```
170.50.1.201 perf760g2.wbem.com perf760g2
```

2. Save the file.

All automatic event handling tasks fail with the following error on the Tasks Results page: Send failed. class Could not connect to SMTP host: ipaddress, port 25;java.net.SocketException: Software caused connection abort:connect.

Solution: If you have antivirus software installed and it is configured to block port 25, configure the antivirus software to unblock port 25 or disable it for the automatic event handling tasks (e-mail) to run correctly.

Tools

I am receiving the HTTP - 404 error when trying to launch a tool.

Solution: This error is received when you try to access any tool that you are not authorized to use.

An mxauthenticationexception is generated when a tool is run from the GUI or the CLI.

Solution:

1. Be sure that you have privileges to run the tool on the system. Refer to "Users and Authorizations" to verify and grant privileges.
2. Be sure that the SSH daemon is accessible on the target system.
 - a. From the CMS, attempt to manually install SSH to the system. There is no need to sign in, but be sure that you can connect.
 - b. Try to log in as an administrative user to a Windows system and as root to an HP-UX or Linux system.
 - c. From an HP-UX or Linux CMS, enter:

```
ssh root@<HP-UX/Linux node>
```

or

```
ssh Administrator@<Windows node>
```

From a Window CMS:

```
<OpenSSH directory>\bin\ssh root@<HP-UX/Linux node>
```

```
<OpenSSH directory>\bin\ssh Administrator@<Windows node>
```

If you are prompted to accept a host key or enter a password, then the SSH daemon is accessible.

3. Run **mxagentconfig** again to verify that the keys are transferred:

```
mxagentconfig -a -n <node name or ipaddress> -u <user> -p <password>
```

4. On the system you are attempting to run tools on, verify the permissions of some directories.

Verify the permission on the home directory of the user name you are using.

- The home directory should have permissions:

```
drwxr-xr-x (755)
```

- The .ssh directory within the home directory should have permissions:

```
drwxr-xr-x (755)
```

- The authorized_keys2 file in the .ssh directory should have permissions:

```
-rw-r--r- or -rwxr-xr-x (644 or 755)
```

- a. To verify these permissions:

- On Windows:

```
Run <OpenSSH Install Directory>\bin\ls -ld <File or directory name>
```

- On HP-UX or Linux:

```
Run ls -ld <File or directory name>
```

- b. To change permissions:

- On Windows:

```
Run <OpenSSH Install Directory>\bin\chmod <Permission number><File or directory name>
```

- On HP-UX or Linux:

```
Run chmod <Permission number> <File or directory name> (Permission number is the number above, for example, 644/755)
```

5. When the command is run, the Execute-as user is listed in the status, which is the user for which you have to run **mxagentconfig**.
6. If execution has worked in the past and is now failing, verify that SSH has been reinstalled on the target system. Reinstalling SSH causes the system to have a different host key. Therefore, SSH can verify that it is the system that it is trying to contact.
 - a. Run **mxagentconfig -r -n system name**
or
Go to the GUI and remove the system host key.
 - b. Remove the lines that refer to the system on which to execute. Remove all references to the system (for example, systemname and systemname.hp.com)
 - c. Alternately, you can also remove the entire `known_hosts` file, which means that SSH registers the keys of every system again the next time it contacts them. This behavior could be a security problem until each system has been contacted.
7. Remove the `.ssh` directory from the home directory of the user on the managed system to ensure that there are no old keys or old permissions that could cause **mxagentconfig** to fail.
8. Run **mxagentconfig** again.

Mxagentconfig fails when trying to authorize a user on a Windows managed system that OpenSSH was not installed by HP SIM.

Solution:

1. Run:

```
sshuser -u <username> -d <domain name> >>
"c:\Progra~1\OpenSSH\etc\passwd"
```

2. Run **mxagentconfig** again.

If **mxagentconfig** still fails, be sure SSH is running by following the steps outlined in step 1.

1. Remove the `.ssh` directory from the home directory of the user on the managed system to ensure that there are no old keys or old permissions that could cause **mxagentconfig** to fail.
2. If none of these work, then manually copy the key. Transfer the file `.dtfSshKey.pub` to the managed system. The file can be found at `/etc/opt/mx/config/sshtools/` on Windows and at `<HP SIM Install Directory>\config\sshtools` on HP-UX and Linux.

- On Windows:

```
Enter <location of .pub file> >> <user home
directory>\.ssh\authorized_keys2.
```

Or enter `hpsimssh` if user's home directory did not exist before running **sshuser**.

- On HP-UX or Linux:

Enter `.cat <location of .pub file> >> ~/.ssh/authorized_keys2`.

After installing HP SIM on a Windows system, I cannot run any of the command line tools. I receiving the following error: %1 is not a valid Win32 application.

Solution: Search the root directory for a folder or file named `Program`. If this file exists, delete it. If this folder exists, rename it or delete it if the folder is empty.

When I use the `mxnodesecurity` command on an HP-UX system to add a system from a different domain, the command does not work properly. For example, if I enter `mxnodesecurity -a -p wbem -c openview\wmi:wmi -n testnode10`, the single backslash between `openview` and `wmi` is missing.

Solution: The UNIX shell environment recognizes the single backslash as an escape character. If you want to add a system from a different domain, add another backslash for it to be recognized. For example, `mxnodesecurity -a -p wbem -c openview\\wmi:wmi -n testnode10`.

When I try to run tools, they fail. This error happens with any tool selected.

Solution: This problem happens if HP SIM is installed on a system without a C drive.

When a tool opens a new window and I click the browser Refresh button, the window closes.

Solution: All windows close if they are manually refreshed using the browser Refresh button because the Refresh operation is indistinguishable from a close operation.

I am a full-configuration-rights user on a Linux or HP-UX system. However, I am receive an exception when I try to run the `mxnodesecurity` command.

Solution: The command must be executed by the root user.

When trying to run tools from the command line, I receive an error, stating that SSH authentication failed.

Solution: If you have renamed the administrator account, edit the TDEF files for each tool, and change the Execute-as user. For example:

1. Navigate to `/System Insight Manager/tools`, and open `mx-tool.xml`.
2. Change the `<execute-as-user>Administrator</execute-as-user>` to the new administrator account name.
3. Save the file.
4. At the DOS prompt, run **command:** `mxtool -m -f mx-tool.xml -x force`. The tool will now run.

You must do this for all of the command line tools.

VCRM

I cannot find a desired software component in HP SIM in its listing of a HP Version Control Repository Manager software catalog. I know it exists in the selected VCRM, but I cannot find it in the displayed list.

Solution: It might be listed as a revision of another component with a slightly different name if the component name has changed since a previous revision. If you still cannot find the component, you might want to browse to the HP Version Control Agent on each individual system and install the component from there.

During the HP Systems Insight Manager (HP SIM) installation, the VCRM fails to install.

Solution:

Use the following method to uninstall the VCRM. Simply reinstalling the VCRM over the existing VCRM might continue to produce the error.

1. Click **Start->Control Panel**.
2. Double-click **Add or Remove Programs**. The **Add or Remove Programs** dialog box appears.
3. Scroll down and select the current **HP Version Control Repository Manager**.
4. Click **Remove** to uninstall the VCRM.
5. Reboot the system, and then reinstall VCRM. For more information regarding installing the VCRM (without using HP SIM), refer to HP Version Control Installation Guide at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

Virtual Machine

JVM is shutting down.

Solution: This could happen if you have physically disconnected the central management server from your network. Restart HP SIM and the problem should correct itself.

VMM

The HP ProLiant Essentials Virtual Machine Management Pack (HP ProLiant Essentials Virtual Machine Management Pack) functions are not working in HP SIM.

Solution: Attempts to log in to the VMM plug-in for HP SIM 4.x will not succeed if the user name contains a character that is not alphanumeric, which prevents the VMM functions from being used within HP SIM.

Windows NT Event Log

If you receive the error message DCOM was unable to communicate with computer<system> using any of the configured protocols, in the Windows NT Event

Log, disable logging the WMI errors. These error messages are not generated by WMIMapper. Rather, they are generated by the Microsoft Windows Management Instrumentation (WMI) service when it cannot communicate with the target system to get the WMI information. Usually, the target system is a non-Windows system.

Solution: To disable logging the WMI errors to the Windows NT Event Log, perform the following procedure on the system where WMIMapper is installed.

1. In Windows NT, click **Control Panel->Administrative Tools->Services**, and stop the **Pegasus WMI Mapper** service.
2. Right-click **My Computer**.
3. Select **Manage**. The **Computer Management** page appears.
4. Expand **Services and Applications**.
5. Right-click **WMI Control**. The **WMI Control Properties** page appears.
6. Select the **Logging** tab.
7. Select **Disabled** from the **Logging level** section, and then click **OK** to close this page.
8. From the **Computer Management** window, double-click **Services**, and then select **Windows Management Instrumentation** service. Stop and restart the service.
9. Start the **Pegasus WMI Mapper** service from the **Services** page.

WMIMapper

The WBEM protocol is not listed on the System Page for the system, and the data from WBEM is not displayed.

Solution: By default, when the CMS is installed on a Windows platform, the WMIMapper service is installed at `c:\Program Files\The Open Group\WMIMapper`. The WMIMapper installation also creates a directory named `c:\hp` (lowercase) with a subfolder containing the certificates used by the system. If you previously created a directory called `c:\HP` (uppercase) the certificates are installed under that directory. When the WBEM and WMIMapper try to communicate, WMIMapper looks for a directory named `c:\hp` (lowercase) and cannot find the certificates. This same problem applies wherever the Windows platform the WMIMapper is installed. To solve this problem, delete the `c:\HP` (uppercase) directory before installing the CMS or WMIMapper on a Windows platform. Be sure to reroute any application using data in that directory to the new directory.

I cannot access WMI information from a client system.

Solution: WMI is configured to allow remote access to accounts in the *administrators* group. If the privileges are reduced to *guest* on the remote system, no WMI connection can be obtained from the remote system. Therefore, the local security policy on the client system might be the problem. Modify the setting.

1. Select **Start->Control Panel->Administrative Tools->Local Security Policy->Local Policies->Security Options**, and select **Network Access: Sharing and security model for local accounts**.
2. Select **Classic - local users authenticate as themselves**.

Reference Information

HP Systems Insight Manager (HP SIM) uses a Microsoft SQL Server 2000 Service Pack 3, MSDE (Windows Install), or PostgreSQL SQL 7.4.x (HP-UX or Linux install) database to store collected event and system data. The database can be on the same system as the management application or on a different system that has network access to the database server. However, configuration of HP SIM database tables cannot be performed on a remote system. HP SIM uses the Java DataBase Connectivity (JDBC) and the Open DataBase Connectivity (ODBC) on Windows systems to communicate with the database.

During installation, the necessary database systems and transaction log systems are created before creating and populating the database.

Caution:



Only the HP SIM application should add or delete from these tables. Any other modifications to these tables cause cache coherency problems for the application.

The database contains:

- Events
- Discovered systems
- System status
- User preferences
- Detailed system information
- Language text (English only)

Important:



You should back up the database on a regular basis and monitor the size of the database to expand it as necessary. Refer to “HP-UX/Linux” and “Windows” for more information.

Reports can be created in Microsoft Access, Excel, Crystal Reports, or any standard reporting tool that can access the database. The database schema is published to make creating the reports easier.

Predefined Views

Several predefined views are shipped with HP SIM. These views can be used to search the database for different information such as data collection information, event data and license data.

Notices_view. This view can be used to list events in the system along with their descriptions. It does not contain the specifics of an event, but it can be useful for some simple reports. It returns the system name, event severity, cleared status, received time, cleared time and event description.

View_deviceAssociations. This view is used in building searches, mainly used internally.

licenseCounts. This view is used to show license count data in the license report.

deviceTypesEnum. This view links the devices_table productType field with an (English) string representing the system type.

deviceSubTypesEnum. This view links the nodeSubTypesEnum table enumOrd field with an (English) string representing the system subtype.

Note:



The database and views are not deleted when you uninstall HP SIM.

Refer to “Reporting Views” to see the available Reporting Views.

Database Tables

The following sections provide the contents of the database. The tables describe the information collected by HP SIM and the database table structures that store the information. The following tables are available:

AuthenticationMethods_values table	CIM_ActiveConnection table	CIM_Chassis table
CIM_ComponentCS table	CIM_ComputerSystemPackage table	CIM_ComputerSystem table
CIM_ControlledBy table	CIM_DeviceSAPImplementation table	CIM_DeviceSoftwareIdentity table
CIM_ElementCapabilities table	CIM_HostedStoragePool table	CIM_IPProtocolEndpoint table
CIM_IPRoute table	CIM_iSCSICapabilities table	CIM_iSCSIConn_TCPProtoEnd table
CIM_iSCSIConnection table	CIM_iSCSISession table	CIM_LogicalDevice table
CIM_LogicalDisk table	CIM_LogicalPortGroup table	CIM_MediaAccessDevice table
CIM_MemberOfCollection table	CIM_NetworkPipeComposition table	CIM_NetworkPort table
CIM_NetworkAdapter table	CIM_OperatingSystem table	CIM_PhysicalElement table
CIM_PhysicalMedia table	CIM_PhysicalMemory table	CIM_PhysicalPackage table
CIM_PortController table	CIM_PowerSupply table	CIM_Process table
CIM_Processor table	CIM_Product table	CIM_ProtoControlAccessesUnit table
CIM_ProtocolControllerForPort table	CIM_ProtocolControllerForUnit table	CIM_ProtocolEndpoint table
CIM_Rack table	CIM_Realizes table	CIM_RemoteServiceAccessPoint table

CIM_SCSIProtocolController table	CIM_SCSIProtocolEndpoint table	CIM_Sensor table
CIM_SoftwareElement table	CIM_SoftwareIdentity table	CIM_StoragePool table
CIM_StorageVolume table	CIM_TCPProtocolEndpoint table	Classifications_values table
ComputerSys_HAP table	ComputerSys_LogicalPortGroup table	ComputerSys_NetworkPort table
ComputerSys_PortController table	ComputerSys_SAP table	ComputerSys_SCSIProtoCont table
ComputerSys_SCSIProtoEndp table	ComputerSys_SoftwareIdent table	ComputerSys_StorageVol table
DB_DeviceInfo table	DB_DeviceInfoEx table	DC_Enclosure table
DC_ProliantHost table	Dedicated_values table	DeviceNames table
Device Extended Attributes database table	Devices table	DeviceProtocolInfo table
ExtentStatus_values table	DeviceSnmpSettings table	HP_Cluster table
HP_Node table	HP_NParCabinet table	HP_NParCell table
HP_NParIOChassis table	HP_NParIOChassisSlot table	HP_NPartition table
HP_NParComplex table	HPUX_BaseKernelParameter table	HPUX_Bundle table
HPUX_DNSService table	HPUX_Fileset table	HPUX_HFS table
HPUX_LogicalVolume table	HPUX_NISServerService table	HPUX_NTPService table
HPUX_PhysicalVolume table	HPUX_Product table	HPUX_VolumeGroup table
IPAddress table	IPProtocolEnd_NetworkPort table	IPXAddress table
NetworkAddresses_values table	NodeSnapshot table	NodeTypesEnum table
NodeSubTypesEnum table	Notices table	NoticeType table
OperationalStatus_CSvalues table	OperationalStatus_NPvalues table	operationalStatus_PCvalues table
OperationalStatus_SVvalues table	PhysicalPackage_Product table	SCSIProtoCont_SCSIProtoEnd table
SCSIProtocolCont_SoftwareId table	SCSIProtoEnd_SCSIProtoEnd table	SCSIProtoEnd_iSCSISession table
SCSIProtoEnd_NetworkPort table	Snapshot table	SPAllocatedFromStoragePool table
SVAllocatedFromStoragePool table	TCPProtoEnd_IPProtoEnd table	

AuthenticationMethods_values table

Column Name	Data Type	Description
AuthenticationMethodId	BIGINT	Uniquely defines this row
AuthenticationMethodsValue	SMALLINT	Used for reporting purposes
AuthenticationMethodsPos	SMALLINT	Used for reporting purposes

CIM_ActiveConnection table

Column Name	Data Type	Description
Antecedent	BIGINT	A ServiceAccessPoint that is configured to communicate and/or is actively communicating with the Dependent SAP. In a unidirectional connection, this is the SAP that is transmitting.
Dependent	BIGINT	A second ServiceAccessPoint that can communicate with the Antecedent SAP. In a unidirectional connection, this is the SAP that is receiving the communication.

CIM_Chassis table

Column Name	Data Type	Description
Chassis_LUID	BIGINT	LUID uniquely defines this row
NodeID	BIGINT	Partly identifies CIM_Chassis
SnapshotID	BIGINT	Partly identifies CIM_Chassis
CreationClassName	NVARCHAR(256)	Partly identifies CIM_Chassis and equates to CIM_Chassis
Tag	NVARCHAR(256)	An arbitrary string that uniquely identifies the Physical Element, serves as the Element key and can contain information such as asset tag or serial number data
dc_ProductID	NVARCHAR(64)	The product ID string of the enclosure and is empty if the enclosure does not report the productID string
dc_SystemCreationClassName	NVARCHAR(256)	If the chassis is part of a rack, then this attribute is CIM_Rack; otherwise, it is CIM_ComputerSystem
dc_SystemName	NVARCHAR(256)	If the chassis is part of a rack, then this attribute is the value of CIM_Rack.Name; otherwise, it is the value of the owning CIM_ComputerSystem.Name
Name	NVARCHAR(256)	A label by which the object is known
ElementName	NVARCHAR(256)	A user-friendly name for the object
Width	real	Inherited from CIM_PhysicalPackage.Width and is the width of the Physical Package in inches
Height	real	Inherited from CIM_PhysicalPackage.Height and is the height of the Physical Package in inches
Depth	real	Inherited from CIM_PhysicalPackage.Depth and is the depth of the Physical Package in inches

Column Name	Data Type	Description
SerialNumber	NVARCHAR(64)	Inherited from CIM_PhysicalElement.SerialNumber and is a manufacturer-allocated number used to identify the Physical Element
PartNumber	NVARCHAR(256)	Inherited from CIM_PhysicalElement.PartNumber and is the part number assigned by the organization responsible for producing or manufacturing the Physical Element
SKU	NVARCHAR(64)	Inherited from CIM_PhysicalElement.SKU and is the stock keeping unit number for this Physical Element
Model	NVARCHAR(64)	Inherited from CIM_PhysicalElement.Model and is the name by which the Physical Element is generally known
Manufacturer	NVARCHAR(256)	Name of the manufacturer of the component
ChassisTypes	SMALLINT	An enumeration of CIM_ChassisTypes. (1 = Other, 2 = Unknown, 3 = Desktop, 4 = Low Profile Desktop, 5 = Pizza Box, 6 = Mini Tower, 7 = Tower, 8 = Portable, 9 = Laptop, 10 = Notebook, 11 = Hand Held, 12 = Docking Station, 13 = All in One, 14 = Sub Notebook, 15 = Space Saving, 16 = Lunch Box, 17 = Main System Chassis, 18 = Expansion Chassis, 19 = SubChassis, 20 = Bus Expansion Chassis, 21 = Peripheral Chassis, 22 = Storage Chassis, 23 = Rack Mount Chassis, 24 = Sealed-Case PC)
TypeDescriptions	NVARCHAR(512)	Additional information about the CIM_Chassis.ChassisTypes
Version	NVARCHAR(64)	Inherited from CIM_PhysicalElement.Version and is a string indicating the version of the Physical Element
OtherIdentifyingInfo	NVARCHAR(512)	Inherited from CIM_PhysicalElement.OtherIdentifyingInfo. Captures additional data, beyond that of Tag information, that could be used to identify a Physical Element (One example is bar code data associated with an Element that also has an asset tag. If only bar code data is available and is uniqueable to be used as an Element key, this property would be NULL and the bar code data used as the class key, in the Tag property)
R_Model	NVARCHAR(256)	A field used by reporting

CIM_ComponentCS table

Column Name	Data Type	Description
GroupComponent	BIGINT	The ComputerSystem that contains and/or aggregates other systems
PartComponent	BIGINT	The contained (Sub)ComputerSystem

CIM_ComputerSystemPackage table

Column Name	Data Type	Description
Antecedent	BIGINT	A field used by reporting
Dependent	BIGINT	A field used by reporting

CIM_ComputerSystem table

Column Name	Data Type	Description
ComputerSystem_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_ComputerSystem
SnapshotID	BIGINT	Partly identifies CIM_ComputerSystem
Name	NVARCHAR(256)	The inherited Name serves as key of a System instance in an enterprise environment
CreationClassName	NVARCHAR(256)	CreationClassName indicates the name of the class or the subclass used in the creation of an instance (When used with the other key properties of this class, this property allows all instances of this class and its subclasses to be uniquely identified.)
Description	NVARCHAR(512)	The Description property provides a textual description of the object
Caption	NVARCHAR(64)	The Caption property is a short textual description (one- line string) of the object
Status	NVARCHAR(10)	Inherited from CIM_ManagedSystemElement.Status and is a string indicating the current status of the object
PrimaryOwnerContact	NVARCHAR(256)	A string that provides information on how the primary system owner can be reached
PrimaryOwnerName	NVARCHAR(64)	The name of the primary system owner
dc_PrimaryOwnerPager	NVARCHAR(32)	Not standard, based on CIM_Person.Pager and includes pager information for the primary owner
dc_SystemLocation	NVARCHAR(256)	Not standard and includes information describing the physical location of this system

Column Name	Data Type	Description
dc_HardwareCapability	NVARCHAR(64)	Not standard and is the hardware capability (32 and 64 bits) of the system
R_OverallStatus	NVARCHAR(50)	A field used by reporting
R_ProductType	NVARCHAR(256)	A field used by reporting
Domain	NVARCHAR(256)	Domain of this system
Elementname	NVARCHAR(256)	A user friendly name for this element
NameFormat	NVARCHAR(64)	Defines how the Name is generated
ReleaseDate	NVARCHAR(256)	For Non-Stop systems, date of system release
R_OperationalStatus	NVARCHAR(256)	A field used by Reporting
R_PortCount	INT	A field used by Reporting
R_PortUtilized	INT	A field used by Reporting

CIM_ControlledBy table

Column Name	Data Type	Description
Dependent	BIGINT	The controlled Device
Antecedent	BIGINT	The controller

CIM_DeviceSAPImplementation table

Column Name	Data Type	Description
deviceSAPImplementation_LUID	BIGINT	Used for reporting purposes
NodeID	BIGINT	Partly identifies CIM_DeviceSAPImplementation
SnapshotID	BIGINT	Partly identifies CIM_DeviceSAPImplementation
Dependent	BIGINT	The ServiceAccessPoint implemented using the LogicalDevice
Antecedent	BIGINT	The LogicalDevice
dc_PermanentAddress	NVARCHAR(256)	Used for reporting purposes

CIM_DeviceSoftwareIdentity table

Column Name	Data Type	Description
System	BIGINT	Used for reporting purposes
InstalledSoftware	BIGINT	Used for reporting purposes

CIM_ElementCapabilities table

Column Name	Data Type	Description
Dependent	BIGINT	The managed element
Antecedent	BIGINT	The Capabilities object associated with the element

CIM_HostedStoragePool table

Column Name	Data Type	Description
GroupComponent	BIGINT	The parent system in the Association
PartComponent	BIGINT	The StoragePool that is a component of a system

CIM_IPProtocolEndpoint table

Column Name	Data Type	Description
IPProtocolEndpoint_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_IPProtocolEndpoint
SnapshotID	BIGINT	Partly identifies CIM_IPProtocolEndpoint
Name	NVARCHAR(1024)	A label by which the object is known
ServiceCreationClassName	NVARCHAR(256)	For future use
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes
IPv4Address	NVARCHAR(255)	The IPv4 address that this ProtocolEndpoint represents

CIM_IPRoute table

Column Name	Data Type	Description
IPRoute_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_IPRoute
SnapshotID	BIGINT	Partly identifies CIM_IPRoute
CreationClassName	NVARCHAR(256)	Equates to CIM_IPRoute
ServiceCreationClassName	NVARCHAR(256)	For future use
ServiceName	NVARCHAR(256)	For future use
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
IPDestinationAddress	NVARCHAR(256)	

Column Name	Data Type	Description
IPDestinationMask	NVARCHAR(256)	The IP address that serves as the destination of the traffic, formatted according to the appropriate convention as defined in the AddressType property of this class (This property has the same semantics as DestinationAddress inherited from the NextHopRouting superclass but uses a different property name because this property and class were defined before NextHopRouting and are Key properties. They cannot be removed. ModelCorrespondence indicates that they should be set to equivalent values for consistency and ease of searching.)
AddressType	SMALLINT	An enumeration that describes the format of the address property (Addresses that can be formatted in IPv4 format must be formatted that way to ensure mixed IPv4/IPv6 support. AddressType is part of the key so that an IPv4 and an IPv6 route to IP subnets with the same network number but different versions (v4/v6) can coexist. (0, Unknown; 2, IPv4; 2 IPv6))
IsStatic	bit	True indicates that this is a static route and False indicates a dynamically-learned route
NextHop	NVARCHAR(256)	Contains the address of the next-hop router or the interface used to reach the destination
	NVARCHAR(32)	Not standard and is the gateway to the route destination (Unknown, Local, Remote)
dc_RouteArgument	NVARCHAR(1024)	Not standard and is the argument list for the <code>/usr/sbin/route</code> command

CIM_iSCSICapabilities table

Column Name	Data Type	Description
ISCSICapabilities_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Used to partially identify CIM_iSCSICapabilities
SnapshotID	BIGINT	Used to partially identify CIM_iSCSICapabilities
Elementname	NVARCHAR(255)	Used for reporting purposes
InstanceID	NVARCHAR(255)	Used for reporting purposes
MinimumSpecificationVersionS	BIT	Used for reporting purposes
MaximumSpecificationVersionS	BIT	Used for reporting purposes

CIM_iSCSIConn_TCPPProtoEnd table

Column Name	Data Type	Description
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes

CIM_iSCSIConnection table

Column Name	Data Type	Description
iSCSIConnection_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_iSCSIConnection
SnapshotID	BIGINT	Partly identifies CIM_iSCSISession
ElementName	NVARCHAR(255)	Used for reporting purposes
InstanceID	NVARCHAR(255)	Used for reporting purposes
ConnectionID	INT	Used for reporting purposes
HeaderDigestMethod	SMALLINT	Used for reporting purposes
OtherheaderDigestMethod	NVARCHAR(255)	Used for reporting purposes
DataDigestMethod	SMALLINT	Used for reporting purposes
OtherDataDigestMethod	NVARCHAR	Used for reporting purposes
ActiveiSCSIVersion	BIT	Used for reporting purposes

CIM_iSCSISession table

Column Name	Data Type	Description
iSCSISession_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_iSCSISession
SnapshotID	BIGINT	Partly identifies CIM_iSCSISession
InstanceID	NVARCHAR(255)	Used for reporting purposes
SessionType	SMALLINT	Used for reporting purposes
TSIH	INT	Used for reporting purposes
EndPointName	NVARCHAR(255)	Used for reporting purposes
CurrentConnections	INT	Used for reporting purposes
ErrorRecoveryLevel	INT	

SCSIProtoEnd_iSCSISession table

Column Name	Data Type	Description
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes

SCSIProtoEnd_NetworkPort table

Column Name	Data Type	Description
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes

CIM_LogicalDevice table

Column Name	Data Type	Description
LogicalDevice_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_LogicalDevice
SnapshotID	BIGINT	Partly identifies CIM_LogicalDevice
DeviceID	NVARCHAR(64)	An address or other identifying information to uniquely name the Logical Device
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_LogicalDevice and equates to CIM_LogicalDevice
ServiceCreationClassName	NVARCHAR(256)	SystemCreationClassName partly identifies CIM_LogicalDevice and equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	SystemName partly identifies CIM_LogicalDevice and is the value of CIM_ComputerSystem.Name with equal NodeID
Name	NVARCHAR(256)	A label by which the object is known
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption and is a short textual description (one line string) of the object
Description	NVARCHAR(512)	A textual description of the object
Availability	SMALLINT	The primary availability and status of the system and is an enumeration. (1 = Other, 2 = Unknown, 3 = Running/Full Power, 4 = Warning, 5 = In Test, 6 = Not Applicable, 7 = Power Off, 8 = Off Line, 9 = Off Duty, 10 = Degraded, 11 = Not Installed, 12 = Install Error, 13 = Power Save, Unknown, 14 = Power Save, Low Power Mode, 15 = Power Save, Standby, 16 = Power Cycle, 17 = Power Save, Warning, 18 = Paused, 19 = Not Ready, 20 = Not Configured, 21 = Quiesced)
LastErrorCode	INT	Captures the last error code reported by the Logical Device
dc_HardwareType	NVARCHAR(64)	Not standard and is the hardware type for this system

Column Name	Data Type	Description
OtherIdentifyingInfo	NVARCHAR(256)	Captures additional data, beyond DeviceID information, that could be used to identify a LogicalDevice. One example would be to hold the Operating System user friendly name for the Device in this property.
dc_AssociatedDriver	NVARCHAR(64)	Not standard and the associated driver for this system

CIM_LogicalDisk table

Column Name	Data Type	Description
LogicalDisk_LUID	BIGINT	LUID uniquely defining this table row
NodeID	INT	Partly identifies CIM_LogicalDisk
Snapshot	INT	Partly identifies CIM_LogicalDisk
DeviceID	NVARCHAR(256)	Inherited from CIM_LogicalDevice.DeviceID and is an address or other identifying information to uniquely name the Logical Device
CreationClassName	NVARCHAR(256)	Equates to CIM_LogicalDisk
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
Win32_FreeSpace	BIGINT	Derived from Win32_LogicalDisk and is the total amount of free space in bytes
Win32_Size	BIGINT	Derived from Win32_LogicalDisk and is the total size in bytes; if unknown, enter 0. Units (bytes)
Description	NVARCHAR(512)	A textual description of the object
R_SizeMB	NVARCHAR(256)	A field used by reporting
R_UsedMB	NVARCHAR(256)	A field used by reporting
R_UsedPercent	NVARCHAR(256)	A field used by reporting
dc_SpaceUsed	BIGINT	Not standard and is the file system space currently in use in bytes
dc_PercentSpaceUsed	INT	Not standard and is the percent of file system space currently in use
BlockSize	BIGINT	Size in bytes of a block on the logical disk.
NumberOfBlocks	BIGINT	Number of storage block in the logical disk; size in bytes can be calculated from $BlockSize * NumberOfBlocks$.

CIM_LogicalPortGroup table

Column Name	Data Type	Description
LogicalPortGroup_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_LogicalPortGroup
Snapshot	BIGINT	Partly identifies CIM_LogicalPortGroup
InstanceID	NVARCHAR(255)	Used for reporting purposes
Name	NVARCHAR(256)	A label by which the object is known
NameFormat	NVARCHAR(64)	Used for reporting purposes
ElementName	NVARCHAR(255)	Used for reporting purposes

CIM_MediaAccessDevice table

Column Name	Data Type	Description
MediaAccessDevice_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_MediaAccessDevice
SnapshotID	BIGINT	Partly identifies CIM_MediaAccessDevice
DeviceID	NVARCHAR(64)	Inherited from CIM_LogicalDevice.DeviceID and is an address or other identifying information to uniquely name the Logical Device
CreationClassName	NVARCHAR(256)	Equates to CIM_MediaAccessDevice
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name for this NodeID
Name	NVARCHAR(256)	A label by which the object is known
Description	NVARCHAR(512)	A textual description of the object
MaxMediaSize	BIGINT	Maximum size, in KB, of media supported by this system. (KB is interpreted as the number of bytes X 1000 not bytes X 1024)
UnitsUsed	BIGINT	An unsigned integer indicating the currently used units of the AccessDevice, helpful to describe when the system might require cleaning (The property UnitsDescription, defines how units should be interpreted)
DefaultBlockSize	BIGINT	Default block size, in bytes
OtherIdentifyingInfo	NVARCHAR(256)	Inherited from CIM_LogicalDevice.OtherIdentifyingInfo (Captures additional data, beyond DeviceID information, that could be used to identify a LogicalDevice. One example would be to hold the Operating System user-friendly name for the Device in this property.)

Column Name	Data Type	Description
TotalPowerOnHours	BIGINT	Inherited from CIM_LogicalDevice.TotalPowerOnHours and is the total number of hours that this Device has been powered
UnitsDescription	NVARCHAR(256)	Defines units relative to its use in the property, MaxUnitsBeforeCleaning; describes the criteria used to determine when the MediaAccessDevice should be cleaned
NeedsCleaning	BIT	Indicates the MediaAccessDevice needs cleaning
Status	NVARCHAR(10)	Inherited from CIM_ManagedSystemElement.Status; a string indicating the current status of the object
MAStatInf_UnrecoverableWriteOp	INT	Corresponds to MediaAccessStatInfo_UnrecoverableWriteOperations. CIM_MediaAccessStatInfo.UnrecoverableWriteOperations; the number of unrecoverable write operations
MAStatInf_UnrecoverableReadOp	INT	Corresponds to MediaAccessStatInfo_UnrecoverableReadOperations. CIM_MediaAccessStatInfo.UnrecoverableReadOperations; the number of unrecoverable read operations
dc_RaidLevel	NVARCHAR(64)	Holds the fault-tolerant RAID setting for a logical drive on a RAID controller (Possible statuses include Not enabled, RAID Level 0, RAID Level 1, RAID Level 0 + 1, Mirroring, Data Guard, Distributed Data Guard (RAID 5), Advanced Data Guarding, RAID Level 4, RAID Level 5)
dc_Type	NVARCHAR(64)	Not standard; a string describing the type of media used to access the system
dc_TransferMode	NVARCHAR(64)	Not standard. Compaq ATA Disk Transfer Mode (othe, pioMode0, pioMode1, pioMode2, pioMode3, pioMode4, dmaMode0, dmaMode1, dmaMode2, ultraDmaMode0, ultraDmaMode1, ultraDmaMode2, ultraDmaMode3, ultraDmaMode4, ultraDmaMode5)
R_DrivePort	NVARCHAR(256)	A field used by reporting
R_Type	NVARCHAR(64)	A field used by reporting

CIM_NetworkAdapter table

Column Name	Data Type	Description
NetworkAdapter_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_NetworkAdapter
SnapshotID	BIGINT	Partly identifies CIM_NetworkAdapter
CreationClassName	NVARCHAR(256)	Equates to CIM_NetworkAdapter
DeviceID	NVARCHAR(64)	Inherited from CIM_LogicalDevice.DeviceID; (an address or other identifying information to uniquely name the Logical Device)
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name for this NodeID
Name	NVARCHAR(256)	A label by which the object is known
NetworkAddress	NVARCHAR(64)	An array of strings indicating the network addresses for an adapte; represented by a comma separated list
StatusInfo	SMALLINT	Inherited from CIM_LogicalDevice.StatusInfo (The StatusInfo property indicates whether the Logical Device is in an enabled (value = 3), disabled (value = 4), other (value = 1), or unknown (value = 2) state. If this property does not apply to the LogicalDevice, the value 5 (Not Applicable), should be used. If a Device is Enabled (value=3), it has been powered up and is configured and operational. The system might not be functionally active, depending on whether its Availability (or AdditionalAvailability) indicates that it is Running/Full Power (value=3) or Off line (value=8). In an enabled but offline mode, a system might be performing out-of-band requests, such as running Diagnostics. If (\ "Disabled\ ") StatusInfo value=4), a device can only be \ "enabled\ " or powered off. In a personal computer environment, (\ "Disabled\ ") means that the system's driver is not viable in the stack. In other environments, a system can be disabled by removing its configuration file. A disabled device is physically present in a system and consuming resources but cannot be communicated with until a load of a driver, a load of a configuration file, or some other \ "enabling\ " activity has occurred. CIM_LogicalDevice.StatusInfo Enumeration. (1 = Other, 2 = Unknown, 3 = Enabled, 4 = Disabled, 5 = Not Applicable)

Column Name	Data Type	Description
PermanentAddress	NVARCHAR(64)	PermanentAddress defines the network address hardcoded into an adapter (This hardcoded address can be changed through firmware upgrade or software configuration. If so, this field should be updated when the change is made. PermanentAddress should be left blank if no hardcoded address exists for the NetworkAdapter.)
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; a short textual description (one line string) of the object
EthernetAdp_InternalMACRcvErr	INT	A count of frames for which reception on a particular interface fails because of an internal MAC sublayer receive error (A frame is only counted by an instance of this object if it is not counted by the corresponding instance of the FrameTooLong property, the AlignmentErrors property, or the FCSErrors property. The precise meaning of the count represented by and instance of this object is implementation-specific. In particular, an instance of this object can represent a count of receive errors on a particular interface that are not otherwise counted.)
EthernetAdp_InternalMACTranErr	INT	A count of frames for which reception on a particular interface fails because of an internal MAC sublayer receive error (A frame is only counted by an instance of this object if it is not counted by the corresponding instance of the LateCollisions property, the Excessive Collisions property, or the CarrierSenseErrors property. The precise meaning of the count represented by and instance of this object is implementation-specific. In particular, an instance of this object can represent a count of transmission errors on a particular interface that are not otherwise counted.)
FullDuplex	BIT	Boolean indicating that the adapter is operating in full duplex mode
OctetsTransmitted	BIGINT	The total number of octets transmitted, including framing characters
OctetsReceived	BIGINT	The total number of octets received, including framing characters
MaxSpeed	BIGINT	The maximum speed, in bits per second, for the Network Adapter

Column Name	Data Type	Description
IPProtocolEndpoint_SubnetMask	NVARCHAR(64)	Derived from CIM_IPProtocolEndpoint.SubnetMask; the mask for the IP address of this ProtocolEndpoint, formatted according to the appropriate convention as defined in the AddressType property of this class
dc_AdminStatus	NVARCHAR(32)	Holds the administrative status of the adapter (For example, Up, Down, Testing, Dormant, Some component missing)
dc_BroadcastAddress	NVARCHAR(64)	Not standard. This attribute is the broadcast address assigned to this interface in dot notation format.
dc_DHCPEnabled	NVARCHAR(32)	Not standard; this attribute indicates whether DHCP enabled or not
dc_OperStatus	NVARCHAR(32)	Holds the operational status for the adapter (For example, Up, Down, Testing)
R_InputErrors	NVARCHAR(256)	A field used by reporting
R_OutputErrors	NVARCHAR(256)	A field used by reporting
R_Duplex	NVARCHAR(25)	A field used by reporting
R_MacAddress	NVARCHAR(64)	A field used by reporting
LANEndpoint_ProtocolType	SMALLINT	Integer indicating protocol active on port: ValueMap { "0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "10", "11", "12", "13", "14", "15", "16", "17", "18", "19", "20", "21", "22", "23", "24", "25", "26", "27" }, Values {"Unknown", "Other", "IPv4", "IPv6", "IPX", "AppleTalk", "DECnet", "SNA", "CONP", "CLNP", "VINES", "XNS", "ATM", "Frame Relay", "Ethernet", "TokenRing", "FDDI", "Infiniband", "Fibre Channel", "ISDN BRI Endpoint", "ISDN B Channel Endpoint", "ISDN D Channel Endpoint", "IPv4/v6", "BGP", "OSPF", "MPLS", "UDP", "TCP" }
LANEndpoint_OperationalStatus	nvarchar(255)	Operational status values for this port
EthernetPort_PortType	SMALLINT	Integer code for port type if Ethernet: ValueMap {"0", "1", "50", "51", "52", "53", "16000..65535"}, Values {"Unknown", "Other", "10BaseT", "10-100BaseT", "100BaseT", "1000BaseT", "Vendor Reserved"}
EthernetPort_MaxDataSize	INT	Max data size of Ethernet packets

CIM_MemberOfCollection table

Column Name	Data Type	Description
Collection	BIGINT	Used for reporting purposes
Member	BIGINT	Used for reporting purposes

CIM_NetworkPipeComposition table

Column Name	Data Type	Description
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes

CIM_NetworkPort table

Column Name	Data Type	Description
NetworkPort_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_NetworkPort
SnapshotID	BIGINT	Partly identifies CIM_NetworkPort
ElementName	NVARCHAR(255)	Used for reporting purposes
Name	NVARCHAR(1024)	A label by which the object is known
SystemCreationClassName	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes
DeviceID	BIGINT	Used for reporting purposes
Speed	BIGINT	Used for reporting purposes
MaxSpeed	BIGINT	Used for reporting purposes
UsageRestriction	SmallInt	Used for reporting purposes
PortType	SMALLINT	Used for reporting purposes
OtherPortType	NVARCHAR(255)	Used for reporting purposes
LinkTechnology	SMALLINT	Used for reporting purposes
OtherLinkTechnology	NVARCHAR(255)	Used for reporting purposes
PermanentAddress	NVARCHAR(64)	Used for reporting purposes
PortNumber	SMALLINT	Used for reporting purposes
R_OperationalStatus	NVARCHAR(256)	Used for reporting purposes
R_ParentName	NVARCHAR(256)	Used for reporting purposes
R_PortType	NVARCHAR(256)	Used for reporting purposes

CIM_OperatingSystem table

Column Name	Data Type	Description
OperatingSystem_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_OperatingSystem
SnapshotID	BIGINT	Partly identifies CIM_OperatingSystem
CSCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem.
CSName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name for this NodeID
CreationClassName	NVARCHAR(256)	Equates to CIM_OperatingSystem.
Name	NVARCHAR(256)	The inherited Name serves as key of an operating system instance within a computer system
LastBootupTime	BIGINT	Time when the OperatingSystem was last booted
LocalDateTime	BIGINT	OperatingSystem notion of the local date and time of day
Version	NVARCHAR(64)	A string describing the OperatingSystem version number (The format of the version information is as follows: <Major Number>..<Minor Number>.<Revision> or <Major Number>.<Minor Number>.<Revision Letter>)
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; a textual description of an object

Column Name	Data Type	Description
OSType	SMALLINT	An integer indicating the type of Operating System (CIM_OSType enumeration. (0 = Unknown, 1 = Other, 2 = MACOS, 3 = ATTUNIX, 4 = DGUX, 5 = DECNT, 6 = Digital Unix, 7 = OpenVMS, 8 = HPUX, 9 = AIX, 10 = MVS, 11 = OS400, 12 = OS/2; 13 = JavaVM, 14 = MSDOS, 15 = WIN3x, 16 = WIN95, 17 = WIN98, 18 = WINNT, 19 = WINCE, 20 = NCR3000, 21 = NetWare, 22 = OSF, 23 = DC/OS, 24 = Reliant UNIX, 25 = SCO UnixWare, 26 = SCO OpenServer, 27 = Sequent, 28 = IRIX, 29 = Solaris, 30 = SunOS, 31 = U6000, 32 = ASERIES, 33 = TandemNSK, 34 = TandemNT, 35 = BS2000, 36 = LINUX, 37 = Lynx, 38 = XENIX, 39 = VM/ESA, 40 = Interactive UNIX, 41 = BSDUNIX, 42 = FreeBSD, 43 = NetBSD, 44 = GNU Hurd, 45 = OS9, 46 = MACH Kernel, 47 = Inferno, 48 = QNX, 49 = EPOC, 50 = IxWorks, 51 = VxWorks, 52 = MiNT, 53 = BeOS, 54 = HP MPE, 55 = NextStep, 56 = PalmPilot, 57 = Rhapsody, 58 = Windows 2000, 59 = Dedicated, 60 = OS/390, 61 = VSE, 62 = TPF, 63 = Windows (R) Me, 64 = Caldera Open UNIX, 65 = OpendBSD, 66 = Not Applicable)
NumberOfUsers	INT	Number of user sessions for which the operating system is currently storing state information
NumberOfProcesses	INT	Number of process contexts currently loaded or running on the operating system
MaxNumberOfProcesses	INT	Max number of process contexts the operating system can support; if no fixed value, then 0
CurrentTimeZone	SMALLINT	Indicates the number of minutes the operating system is offset from GMT; the number is +, -, or 0
TotalVisibleMemorySize	BIGINT	Amount of physical memory in KB available to operating system; not necessarily true amount of physical memory but what is reported to the operating system as available
TotalSwapSpaceSize	BIGINT	Total swap space in Kb; can be null if swap space is not distinguished from page files

Column Name	Data Type	Description
OtherTypeDescription	NVARCHAR(64)	A string describing the manufacturer and operating system type; used when the OperatingSystem property, OSType, is set to 1 or 59 (Other or Dedicated) (The format of the string inserted in OtherTypeDescription should be similar in format to the Values strings defined for OSType. OtherTypeDescription should be set to null when OSType is any value other than 1 or 59.)
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; a short textual description (one line string) of the object
dc_OperatingSystemCapability	NVARCHAR(64)	Not Standard; the capability (32 and 64 bits) of this operating system
dc_OSType	NVARCHAR(256)	Not standard; a string describing the operating system type (This can involve interpretation and not strictly reflect the value of OSType.)
dc_PrimaryOS	bit	Not standard; derived from CIM_InstalledOSBoolean indicating that the OS is the default for the Computer System
Win32_CSDVersion	NVARCHAR(256)	Not standard; CSD version/Service Pack level of OS from Windows systems
dc_SwapSpaceName	NVARCHAR(256)	Not standard. Name identifying the swap space.
dc_SwapType	NVARCHAR(64)	Not standard; type description of swap space
dc_SwapSpaceMinimumSize	BIGINT	Not standard. Minimum size of swap space
dc_SwapSpaceMaximumSize	BIGINT	Not standard; maximum size of swap space
dc_SwapSpaceReservedSize	BIGINT	Not standard; reserved size of swap space

CIM_PhysicalElement table

Column Name	Data Type	Description
PhysicalElement_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_PhysicalElement
SnapshotID	BIGINT	Snapshot partly identifies CIM_PhysicalElement
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_PhysicalElement; equates to CIM_PhysicalElement

Column Name	Data Type	Description
Tag	NVARCHAR(256)	Tag partly identifies CIM_PhysicalElement; an arbitrary string that uniquely identifies the Physical Element and serves as the Element's key and can contain information such as asset tag or serial number data
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; a short textual description (one line string) of the object
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; a textual description of an object
Name	NVARCHAR(256)	The label by which this object is known
InstallDateTime	BIGINT	Inherited from CIM_ManagedSystemElement.InstallDate; a datetime value indicating when the object was installed; a lack of a value does not indicate that the object is not installed
Status	NVARCHAR(10)	Inherited from CIM_ManagedSystemElement.Status; a string indicating the current status of the object
ManufactureDate	BIGINT	Date this physical element was manufactured
Manufacturer	NVARCHAR(256)	The name of the organization responsible for producing the Physical Element (This can be the entity from which the element is purchased, but this is not necessarily true. The latter information is contained in the Vendor property of CIM_Product.)
Model	NVARCHAR(64)	The name by which the Physical Element is generally known
OtherIdentifyingInfo	NVARCHAR(512)	Captures additional data, beyond that of Tag information, that could be used to identify a Physical Element (One example is bar code data associated with an Element that also has an asset tag. Note that if only bar code data is available and is unique or able to be used as an Element key, this property would be null and the bar code data used as the class key in the Tag property.)
PartNumber	NVARCHAR(256)	The part number assigned by the organization responsible for producing or manufacturing the Physical Element
PoweredOn	bit	Boolean value indicating that the Physical Element is powered on (true), or is currently off (false)

Column Name	Data Type	Description
SerialNumber	NVARCHAR(64)	A manufacturer-allocated number used to identify the Physical Element
SKU	NVARCHAR(64)	The stock keeping unit number for this Physical Element
Version	NVARCHAR(64)	A string indicating the version of the Physical Element
Slot_Number	SMALLINT	The Number property indicates the physical slot number, which can be used as an index into a system slot table, whether that slot is physically occupied
dc_Location	NVARCHAR(64)	Not standard; a string describing the location of the physical element
dc_Condition	NVARCHAR(64)	Not standard; a string describing the condition of the physical element such as OK, Degraded, or Failed
dc_FirmwareRevision	NVARCHAR(64)	Not standard; a firmware revision associated with the physical element
dc_HWLocation	NVARCHAR(256)	Not standard; a text description of the hardware location, on complex multi-SBB hardware only, for the element
dc_ProductID	NVARCHAR(64)	The product ID string of the server blade

CIM_PhysicalMedia table

Column Name	Data Type	Description
PhysicalMedia_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_PhysicalMedia
SnapshotID	BIGINT	Snapshot partly identifies CIM_PhysicalMedia
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_PhysicalMedia; equates to CIM_PhysicalMedia
Tag	NVARCHAR(256)	Inherited from CIM_PhysicalElement.Tag; an arbitrary string that uniquely identifies the Physical Element and serves as the Element's key, can contain information such as asset tag or serial number data

Column Name	Data Type	Description
MediaType	SMALLINT	<p>Specifies the type of the PhysicalMedia, as an enumerated integer (The MediaDescription property is used to provide more explicit definition of the Media type, whether it is pre-formatted, compatability features and so on. CIM_PhysicalMedia.MediaType enumeration. 0 = Unknown, 1 = Other, 2 = Tape, 3 = QIC Cartridge, 4 = AIT Cartridge, 5 = DTF Cartridge, 6 = DAT Cartridge, 7 = 8mm Tape Cartridge, 8 = 19mm Tape Cartridge, 9 = DLT Cartridge, 10 = Half-Inch Magnetic Tape Cartridge, 11 = Cartridge Disk, 12 = JAZ Disk, 13 = ZIP Disk, 14 = SyQuest Disk, 15 = Winchester Removable Disk, 16 = CD_ROM, 17 = CD_ROM/XA, 18 = CD-I; 19, 19 = Recordable, 20 = WORM, 21 = Magento-Optical, 22 = DVD, 23 = DVD-RW+, 24 = DVD-RAM, 25 = DVD-ROM, 26 = DVD-Video, 27 = Divx, 28 = Floppy/Diskette, 29 = Hard Disk, 30 = Memory Card, 31 = Hard Copy, 32 = Clik Disk, 33 = CD-RW, 34 = CD-DA, 35 = CD+, 36 = DVD Recordable, 37 = DVD-RW, 38 = DVD-Audio, 39 = DVD-5, 40 = DVD-9, 41 = DVD-10, 42 = DVD-18, 43 = Magneto-Optical Rewriteable, 44 = Magneto-Optical Write Once, 45 = Magneto-Optical Rewriteable (LIMDOW), 46 = Phase Change Write Once, 47 = Phase Change Rewriteable, 48 = Phase Change Dual Rewriteable, 49 = Ablative Write Once, 50 = Near Field Recording, 51 = MiniQic, 52 = Travan, 53 = 8mm Metal Particle, 54 = 8mm Advanced Metal Evaporate, 55 = NCTP, 56 = LTO Ultrium, 57 = LTO Accelis, 58 = 9 Track Tape, 59 = 18 Track Tape, 60 = 36 Track Tape, 61 = Magstar 3590, 62 = Magstar MP, 63 = D2 Tape, 64 = Tape, DST Small , 65 = Tape, DST Medium, 66 = Tape, DST Large)</p>
Capacity	BIGINT	<p>The number of bytes that can be read from or written to a Media (This property is not applicable to \"Hard Copy\" (documentation) or cleaner Media. Data compression should not be assumed because it would increase the value in this property. For tapes, it should be assumed that no filemarks or blank space areas are recorded on the Media.)</p>

Column Name	Data Type	Description
Removable	bit	Inherited from CIM_PhysicalComponent.Removable (A PhysicalComponent is Removable if it is designed to be taken in and out of the physical container in which it is normally found, without impairing the function of the overall packaging. A component can still be Removable if power must be off to perform the removal. If power can be on and the component removed, then the element is both Removable and HotSwappable. For example, an upgradeable processor chip is removable.)
OtherIdentifyingInfo	NVARCHAR (512)	Captures additional data, beyond that of Tag information, that could be used to identify a Physical Element (One example is bar code data associated with an Element that also has an asset tag. Note that if only bar code data is available and is unique or able to be used as an Element key, this property would be null and the bar code data used as the class key in the Tag property.)
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; a textual description of an object
Name	NVARCHAR(256)	The label by which this object is known
HotSwappable	bit	Inherited from CIM_PhysicalComponent.HotSwappable; (Is HotSwappable if it is possible to replace the Element with a physically different but equivalent one while the containing package has power applied to it (for example, is on))
Manufacturer	NVARCHAR(256)	The name of the organization responsible for producing the Physical Element (This can be the entity from whom the element is purchased, but this is not necessarily true. The latter information is contained in the Vendor property of CIM_Product.)
Model	NVARCHAR(64)	The name by which the Physical Element is generally known
SerialNumber	NVARCHAR(64)	A manufacturer-allocated number used to identify the Physical Element
Version	NVARCHAR(256)	A string indicating the version of the Physical Element

CIM_PhysicalMemory table

Column Name	Data Type	Description
PhysicalMemory_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	
SnapshotID	BIGINT	
CreationClassName	NVARCHAR(256)	CreationClassName identifies CIM_PhysicalMemory; equates to CIM_PhysicalMemory
Tag	NVARCHAR(256)	Tag partly identifies CIM_PhysicalMemory; inherited from CIM_PhysicalElement.Tag; an arbitrary string that uniquely identifies the Physical Element and serves as the Element's key and can contain information such as asset tag or serial number data
MemoryType	SMALLINT	The type of physical memory (CIM_PhysicalMemory.MemoryType Enumeration. 0 = Unknown, 1 = Other, 2 = DRAM, 3 = Synchronous DRAM, 4 = Cache DRAM, 5 = EDO, 6 = EDRAM, 7 = VRAM, 8 = SRAM, 9 = RAM, 10 = ROM, 11 = Flash, 12 = EEPROM, 13 = FEPRAM, 14 = EPROM, 15 = CDRAM, 16 = 3DRAM, 17 = SDRAM, 18 = SGRAM, 19 = RDRAM, 20 = DDR)
Capacity	BIGINT	The total capacity of this PhysicalMemory in bytes
R_MemoryType	NVARCHAR(256)	A field used by reporting
R_MemoryTech	NVARCHAR(256)	A field used by reporting
FormFactor	SMALLINT	Derived from CIM_Chip (The implementation form factor for the Chip. CIM_PhysicalMemory.FormFactor enumeration. 0 = Unknown, 1 = Other, 2 = SIP, 3 = DIP, 4 = ZIP, 5 = SOJ, 6 = Proprietary, 7 = SIMM, 8 = DIMM, 9 = TSOP, 10 = PGA, 11 = RIMM, 12 = SODIMM, 13 = SRIMM, 14 = SMD, 15 = SSMP, 16 = QFP, 17 = TQFP, 18 = SOIC, 19 = LCC, 20 = PLCC, 21 = BGA, 22 = FPBGA, 23 = LGA)
PartNumber	NVARCHAR(256)	The part number assigned by the organization responsible for producing or manufacturing the Physical Element
SerialNumber	NVARCHAR(64)	A manufacturer-allocated number used to identify the Physical Element
dc_ErrorMethodology	NVARCHAR(512)	Not standard; the main error correction scheme supported by this memory component

Column Name	Data Type	Description
dc_HWLocation	NVARCHAR(256)	Not standard; a text description of the hardware location, on complex multi-SBB hardware only, for the memory element
R_Slot	SMALLINT	A field used by reporting
Description	NVARCHAR(64)	Description of the element
BankLabel	nvarchar(64)	Memory bank designator
MemLoc_LocationIdentifiers	nvarchar(255)	Location identifiers for memory on boards

CIM_PhysicalPackage table

Column Name	Data Type	Description
PhysicalPackage_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	System partly identifies CIM_PhysicalPackage
SnapshotID	BIGINT	Snapshot partly identifies CIM_PortController
ElementName	NVARCHAR(255)	Used for reporting purposes
Name	NVARCHAR(1024)	A label by which the object is known
Tag	NVARCHAR(256)	Used for reporting purposes
CreationClassName	NVARCHAR(256)	Used for reporting purposes
Manufacturer	NVARCHAR(64)	Used for reporting purposes
Model	NVARCHAR(256)	Used for reporting purposes
PartNumber	NVARCHAR(256)	Used for reporting purposes

CIM_PortController table

Column Name	Data Type	Description
PortController_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_PortController
SnapshotID	BIGINT	Snapshot partly identifies CIM_PortController
ElementName	NVARCHAR(255)	Used for reporting purposes
SystemCreationClassName	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes
DeviceID	NVARCHAR(64)	Used for reporting purposes
ProtocolSupported	SMALLINT	Used for reporting purposes
R_OperationalStatus	NVARCHAR(256)	Used for reporting purposes
R_PortCount	INT	INT
R_PortUtilized	INT	Used for reporting purposes
R_Condition	NVARCHAR(256)	A field used by reporting

Column Name	Data Type	Description
R_MaxCapacity	NVARCHAR(256)	A field used by reporting
dc_RedundancyState	NVARCHAR(512)	Not standard; The redundancy state of the power supply
dc_CurrentOutputPower	INT	Not standard; capacity and or output power of the power supply in watts

CIM_PowerSupply table

Column Name	Data Type	Description
PowerSupply_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_PowerSupply
SnapshotID	BIGINT	Snapshot partly identifies CIM_PowerSupply
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_PowerSupply; equates to CIM_PowerSupply
DeviceID	NVARCHAR(64)	DeviceID partly identifies CIM_PowerSupply; inherited from CIM_LogicalDevice.DeviceID; an address or other identifying information to uniquely name the Logical Device
SystemCreationClassName	NVARCHAR(256)	SystemCreationClassName partly identifies CIM_PowerSupply (When related data is in CIM_PhysicalElement, this field equates to CIM_PhysicalElement. Otherwise, CIM_ComputerSystem.)
SystemName	NVARCHAR(256)	The value of CIM_PhysicalElement.Name or CIM_ComputerSystem.Name where NodeID is equal.
Name	NVARCHAR(256)	A label by which the object is known

Column Name	Data Type	Description
Availability	SMALLINT	<p>The primary availability and status of the System (Additional status information can be specified using the AdditionalAvailability array property. For example, the Availability property indicates that the System is running and has full power (value=3) or is in a warning (value = 4), test (value = 5), degraded (value = 10), or power save state (values 13-15 and 17). Regarding the Power Save states, these are defined as follows: Value 13 (\ "Power Save - Unknown\ ") indicates that the system is known to be in a power save mode, but its exact status in this mode is unknown; value 14 (\ "Power Save - Low Power Mode\ ") indicates that the system is in a power save state but still functioning and might exhibit degraded performance; value 15 (\ "Power Save - Standby\ ") describes that the system is not functioning but could be brought to full power quickly; and value 17 (\ "Power Save - Warning\ ") indicates that the system is in a warning state, though also in a power save mode.</p> <p>CIM_LogicalDevice.Availability enumeration. 1 = Other, 2 = Unknown, 3 = Running/Full Power, 4 = Warning, 5 = In Test, 6 = Not Applicable, 7 = Power Off, 8 = off Line, 9 = Off Duty, 10 = Degraded, 11 = Not Installed, 12 = Install Error, 13 = Power Save - Unknown, 14 = Power Save - Low Power Mode, 15 = Power Save - Standby, 16 = Power Cycle, 17 = Power Save - Warning, 18 = Paused, 19 = Not Ready, 20 = Not Configured, 21 = Quiesced)</p>

Column Name	Data Type	Description
AdditionalAvailability	SMALLINT	Additional availability and status of the device, beyond that specified in the Availability property (The property denotes the primary status and availability of the device. In some cases, this is not sufficient to denote the complete status of the device. In those cases, the AdditionalAvailability property can be used to provide further information. For example, a device primary Availability might be \"Off line\" (value=8), but it might also be in a low power state (AdditionalAvailability value=14), or the device could be running Diagnostics (AdditionalAvailability value=5, \"In Test\"). See CIM_PowerSupply.Availability enumeration.)
TotalOutput	INT	Represents the total output power of the PowerSupply in milliWatts; 0 denotes Unknown units (milliWatts)
OtherIdentifyingInfo	NVARCHAR(256)	Additional information that can identify the power supply
R_Status	NVARCHAR(256)	A field used by reporting
R_Condition	NVARCHAR(256)	A field used by reporting
R_MaxCapacity	NVARCHAR(256)	A field used by reporting
dc_PowerSupplyPresent	NVARCHAR(32)	Not standard; indicates whether the power supply is present in the chassis
dc_PowerSupplyStatus	NVARCHAR(64)	The status of the power supply (noError (1), generalFailure (2), bistFailure 32), fanFailure (4), tempFailure (5), interlockOpen (6), epromFailed (7), vrefFailed (8), dacFailed (9), ramTestFailed (10), voltageChannelFailed (11), orringdiodeFailed (12), brownOut (13), giveupOnStartup (14), nvramInvalid (15), calibrationTableInvalid (16))
dc_RedundancyState	NVARCHAR(512)	Not standard; the redundancy state of the power supply
dc_CurrentOutputPower	INT	Not standard; capacity and or output power of the power supply in watts

CIM_Process table

Column Name	Data Type	Description
Process_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_Process

Column Name	Data Type	Description
SnapshotID	BIGINT	Snapshot partly identifies CIM_ProcessM/para
CSCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
CSName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name where NodeID is equal
OSCreationClassName	NVARCHAR(256)	OSCreationClassName partly identifies CIM_Process. Equates to CIM_OperatingSystem
OSName	NVARCHAR(256)	OSName partly identifies CIM_Process; the value of CIM_OperatingSystem.Name where NodeID is equal
Handle	NVARCHAR(256)	Handle partly identifies CIM_Process; a string used to identify the Process. A Process ID is a kind of Process Handle
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_Process; equates to CIM_Process
Name	NVARCHAR(256)	Name partly identifies CIM_Process; the name of the process
ExecutionState	SMALLINT	Indicates the current operating condition of the Process; CIM_Process.ExecutionState enumeration (0 = Unknown, 1 = Other, 2 = Ready, 3 = Running, 4 = Suspended Blocked, 6 = Suspended Ready, 7 = Terminated, 8 = Stopped, 9 = Growing)
Priority	INT	Priority indicates the urgency or importance of execution of a Process
UnixProcess_ParentProcessID	NVARCHAR(256)	Derived from CIM_UnixProcess.ParentProcessID; the parent process ID of this executing process
UnixProcess_ProcessGroupID	BIGINT	Derived from CIM_UnixProcess.ProcessGroupID; the group ID of the currently executing process
UnixProcess_RealUserID	BIGINT	Derived from CIM_UnixProcess.RealUserID; the real user id of the currely executing process
UnixProcess_ProcessTTY	NVARCHAR(32)	Derived from CIM_UnixProcess.ProcessTTY; the TTY currently associated with this process
UnixProcess_ModulePath	NVARCHAR(512)	Derived from CIM_UnixProcess.ModulePath; the file path to the executing module for the process
OtherExecutionDescription	NVARCHAR(512)	Derived from CIM_UnixProcess.ModulePath; the executing process command path
UnixProcess_Parameters	NVARCHAR(512)	A string describing the state - used when the instance's ExecutionState property is set to Other; else this field is null

Column Name	Data Type	Description
UnixProcess_ProcessNiceValue	INT	Derived from CIM_UnixProcess.Parameters; the operating system parameters provided to the executing process
UxPrStatInf_RealStack	BIGINT	Derived from CIM_UnixProcess.ProcessNiceValue; the process nice value; used to compute its priority
UxPrStatInf_VirText	BIGINT	UnixProcessStatisticalInformation_RealStack; derived from CIM_UnixProcessStatisticalInformation.RealStack; the number of KB of real stack space used by the process
UxPrStatInf_VirData	BIGINT	UnixProcessStatisticalInformation_VirtualText; derived from CIM_UnixProcessStatisticalInformation.VirtualText; The number of KB of virtual text space used by the process
UxPrStatInf_VirStack	BIGINT	UnixProcessStatisticalInformation_VirtualData; derived from CIM_UnixProcessStatisticalInformation.VirtualData; the number of KB of virtual data space used by the process
UxPrStatInf_VirSharedMem	BIGINT	UnixProcessStatisticalInformation_VirtualStack; derived from CIM_UnixProcessStatisticalInformation.VirtualStack; the number of KBs of virtual stack space used by the process
UxPrStatInf_VirSharedMem	BIGINT	UnixProcessStatisticalInformation_VirtualSharedMemory; derived from CIM_UnixProcessStatisticalInformation.VirtualSharedMemory; the number of KB of shared memory used by the process
UxPrStatInf_VirMemMapFileSize	BIGINT	UnixProcessStatisticalInformation_VirtualMemoryMappedFileSize; derived from CIM_UnixProcessStatisticalInformation.VirtualMemoryMappedFileSize; the number of KB of virtual space used for memory mapped files by the process.

CIM_Processor table

Column Name	Data Type	Description
Processor_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_Processor
SnapshotID	BIGINT	Snapshot partly identifies CIM_Processor
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_Processor; equates to CIM_Processor

Column Name	Data Type	Description
DeviceID	NVARCHAR(64)	DeviceID partly identifies CIM_Processor; inherited from CIM_LogicalDevice.DeviceID; an address or other identifying information to uniquely name the Logical Device
Name	NVARCHAR(256)	Name partly identifies CIM_Processor; a label by which the object is known
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem.
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name where NodeID is equal

Column Name	Data Type	Description
Family	SMALLINT	<p>The Processor Family Type.</p> <p>CIM_Processor.Family enumeration (1 = Other, 2 = Unknown, 3 = 8086, 4 = 80286, 5 = 80386, 6 = 80486, 7 = 8087, 8 = 80287, 9 = 80387, 10 = 80487, 11 = Intel® Pentium® brand, 12 = Pentium® Pro, 13 = Pentium® II, 14 = Pentium® processor with MMX™ technology, 15 = Celeron®, 16 = Pentium® II Xeon™, 17 = Pentium® III, 18 = M1 Family, 19 = M2 Family, 24 = K5 Family, 25 = K6 Family, 26 = K6-2, 27 = K6-3, 28 = AMD Athlon Processor Family, 29 = AMD Duron Processor, 30 = AMD29000 Family, 31 = K6-2+, 32 = Power PC Family, 33 = Power PC 601, 34 = Power PC 603, 35 = Power PC 603+, 36 = Power PC 604, 37 = Power PC 620, 38 = Power PC X704, 39 = Power PC 750, 48 = Alpha Family, 49 = Alpha 21064, 50 = Alpha 21066, 51 = Alpha 21164, 52 = Alpha 21164PC, 53 = Alpha 21164a, 54 = Alpha 21264, 55 = Alpha 21364, 64 = MIPS Family, 65 = MIPS R4000, 66 = MIPS R4200, 67 = MIPS R4400, 68 = MIPS R4600, 69 = MIPS R10000, 80 = SPARC Family, 81 = SuperSPARC, 82 = microSPARC, 83 = microSPARC IIep, 84 = UltraSPARC, 85 = UltraSPARC II, 86 = UltraSPARC Ili, 87 = UltraSPARC III, 88 = UltraSPARC Ilii, 96 = 68040, 97 = 68xxx Family, 98 = 68000, 99 = 68010, 100 = 68020, 101 = 68030, 112 = Hobbit Family, 120 = Crusoe TM5000 Family, 121 = Crusoe TM3000 Family, 128 = Weitek, 130 = Intel® Itanium® Processor, 144 = PA-RISC Family, 145 = PA-RISC 8500, 146 = PA-RISC 8000, 147 = PA-RISC 7300LC, 148 = PA-RISC 7200, 149 = PA-RISC 7100LC, 150 = PA-RISC 7100, 160 = V30 Family, 176 = Pentium® III Xeon™, 177 = Pentium® III Processor with Intel® SpeedStep Technology, 178 = Pentium® 4, 179 = Intel® Xeon™, 180 = AS400 Family, 181 = Intel Xeon processor MP, 190 = K7, 200 = Intel® Xeon™ processor MP, 201 = G4, 202 = G5, 250 = i860, 251 = i960, 260 = SH-3, 261 = SH-4, 280 = ARM, 281 = StrongARM, 300 = 6x86, 301 = MediaGX, 302 = MII, 320 = WinChip, 350 = DSP, 500 = Video Processor)</p>

Column Name	Data Type	Description
CurrentClockSpeed	INT	The current speed (in MHz) of this Processor
UniqueID	NVARCHAR(256)	A globally unique identifier for the processor (This identifier might only be unique within a processor family.)
LoadPercentage	SMALLINT	Loading of this processor, averaged over the last minute in percent
CPUStatus	SMALLINT	The CPUStatus property indicates the current status of the processor (For example, it might be disabled by the user through BIOS (value=2), or disabled because of a POST error (value=3). Information in this property can be obtained from SMBIOS, the Type 4 structure, the Status attribute. CIM_Processor.CPUStatus Enumeration. (0 = Unknown, 1 = CPU, 2 = CPU disabled by user through BIOS setup, 3 = CPU disabled by BIOS (POST error), CPU Is Idle, Other)
OtherIdentifyingInfo	NVARCHAR(64)	Inherited from CIM_LogicalDevice.OtherIdentifyingInfo. OtherIdentifyingInfo captures additional data, beyond DeviceID information, that could be used to identify a LogicalDevice (One example would be the socket and slot information for this processor.)
R_CPUType	NVARCHAR(256)	A field used by reporting
R_CPUSpeed	NVARCHAR(256)	A field used by reporting
R_CPUStatus	NVARCHAR(256)	A field used by reporting
dc_HWLocation	NVARCHAR(256)	Not standard; a text description of the hardware location, on complex multi-SBB hardware only for the processor
ArchitectureRevision	SMALLINT	Architecture revision of the processor
FirmwareRevision	NVARCHAR(255)	Firmware revision of the processor
DataWidth	SMALLINT	Width of the processor datapath in bits
ProcessorLocation_CellNumber	NVARCHAR(255)	Cell in the complex containing this processor (Cellular systems only)

CIM_Product table

Column Name	Data Type	Description
Product_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_Product
SnapshotID	BIGINT	Snapshot partly identifies CIM_Product

Column Name	Data Type	Description
Elementname	NVARCHAR(255)	Used for reporting purposes
Name	NVARCHAR(256)	A label by which the object is known
IdentifyingNumber	NVARCHAR(64)	Product identification
Vendor	NVARCHAR(256)	The name of the Product's supplier or entity selling the product
Version	NVARCHAR(64)	Product version information; corresponds to the Version property in the Product object in the DMTF Solution Exchange Standard

CIM_RemoteServiceAccessPoint table

Column Name	Data Type	Description
RemoteServiceAccessPoint_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_RemoteServiceAccessPoint
SnapshotID	BIGINT	Snapshot partly identifies CIM_RemoteServiceAccessPoint
ElementName	NVARCHAR(255)	Used for reporting purposes
SystemCreationClassName	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
AccessInfo	NVARCHAR(255)	Used for reporting purposes
CreationClassName	NVARCHAR(256)	Used for reporting purposes
Name	NVARCHAR(1024)	A label by which the object is known

CIM_SCSIProtocolController table

Column Name	Data Type	Description
SCSIProtocolController_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_SCSIProtocolController
SnapshotID	BIGINT	Snapshot partly identifies CIM_SCSIProtocolController
ElementName	NVARCHAR(255)	Used for reporting purposes
SystemCreationClassName	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes
DeviceID	NVARCHAR(256)	Used for reporting purposes
MaxUnitsControlled	INT	Used for reporting purposes

CIM_SCSIProtocolEndpoint table

Column Name	Data Type	Description
SCSIProtocolEndpoint_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_SCSIProtocolEndpoint
SnapshotID	BIGINT	Snapshot partly identifies CIM_SCSIProtocolEndpoint
Name	NVARCHAR(1024)	A label by which the object is known
SystemCreationClassName	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes
ConnectionType	SMALLINT	Used for reporting purposes

CIM_ProtoControlAccessesUnit table

Column Name	Data Type	Description
ProtoControlAccessUnit_LUID	BIGINT	Used for reporting purposes
ProtoControlAccessUnit_LUID	BIGINT	Used for reporting purposes

CIM_ProtocolControllerForPort table

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes
NodeID	BIGINT	Node partly identifies CIM_ProtocolControllerForUnit
SnapshotID	BIGINT	Snapshot partly identifies CIM_ProtocolControllerForUnit
DeviceNumber	NVARCHAR(255)	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes
Name	NVARCHAR(255)	A label by which the object is known

CIM_ProtocolControllerForUnit table

Column Name	Data Type	Description
ProtocolControllerForUnit_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_ProtocolControllerForUnit
SnapshotID	BIGINT	Snapshot partly identifies CIM_ProtocolControllerForUnit

Column Name	Data Type	Description
DeviceNumber	NVARCHAR(255)	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes

CIM_ProtocolEndpoint table

Column Name	Data Type	Description
protocolEndpoint_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_ProtocolEndpoint
SnapshotID	BIGINT	Snapshot partly identifies CIM_ProtocolEndpoint
Name	NVARCHAR(1024)	Used for reporting purposes
SystemCreationClassname	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes
ProtocolIFType	NVARCHAR(256)	Used for reporting purposes

CIM_Rack table

Column Name	Data Type	Description
Rack_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_Rack
SnapshotID	BIGINT	Snapshot partly identifies CIM_Rack
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_Rack; equates to CIM_Rack
Tag	NVARCHAR(256)	Tag partly identifies CIM_Rack; inherited from CIM_PhysicalElement.Tag; an arbitrary string that uniquely identifies the Physical Element and serves as the Element key and can contain information such as asset tag or serial number data
SerialNumber	NVARCHAR(64)	Inherited from CIM_PhysicalElement.SerialNumber; a manufacturer-allocated number used to identify the Physical Element
Name	NVARCHAR(256)	A label by which the object is known

CIM_Realizes table

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes

Column Name	Data Type	Description
Antecedent	BIGINT	Used for reporting purposes

CIM_Sensor table

Column Name	Data Type	Description
Sensor_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_Sensor
SnapshotID	BIGINT	Snapshot partly identifies CIM_Sensor
DeviceID	NVARCHAR(64)	DeviceID partly identifies CIM_Sensor; inherited from CIM_LogicalDevice.DeviceID;. an address or other identifying information to uniquely name the Logical Device
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_Sensor; Equates to CIM_Sensor
SystemCreationClassName	NVARCHAR(256)	SystemCreationClassName partly identifies CIM_Sensor (If the sensor is owned by a chassis, then this field equates to CIM_Chassis; otherwise it is set to CIM_ComputerSystem.)
SystemName	NVARCHAR(256)	Equates to CIM_Sensor.Name or CIM_ComputerSystem.Name where NodeID is equal
Name	NVARCHAR(256)	Name partly identifies CIM_Sensor; a label by which the object is known
Status	NVARCHAR(10)	Inherited from CIM_ManagedSystemElement.Status; a string indicating the current status of the object
CurrentState	NVARCHAR(128)	The current state indicated by the Sensor (This is always one of the Possible States property.)
PossibleStates	NVARCHAR(512)	Possible States enumerates the string outputs of the Sensor (For example, a switch sensor can output the states On or Off. Another implementation of the Switch can output the states Open and Close. Another example is a NumericSensor supporting thresholds. This Sensor can report the states like Normal, Upper Fatal, Lower non-critical and so on. A Numeric Sensor that does not publish readings and threshold but stores this data internally can still report its states.)
CurrentReading	INT	The current air temperature at the exhaust of the power supply in degrees Celsius
OtherCurrentReading	INT	The current air temperature at the intake of the power supply in degrees Celsius

Column Name	Data Type	Description
BaseUnit	INT	Code for the units used by the readings (pull from CIM_NumericSensor)
SensorType	SMALLINT	Type of sensor: ValueMap { "0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "10", "11", "12" }, Values { "Unknown", "Other", "Temperature", "Voltage", "Current", "Tachometer", "Counter", "Switch", "Lock", "Humidity", "Smoke Detection", "Presence", "Air Flow" }

CIM_SoftwareElement table

Column Name	Data Type	Description
SoftwareElement_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_SoftwareElement
SnapshotID	BIGINT	Snapshot partly identifies CIM_SoftwareElement
SoftwareElementID	NVARCHAR(256)	SoftwareElementID partly identifies CIM_SoftwareElement (This is an identifier for the Software Element and is designed to be used in conjunction with other keys to create a unique representation of the element.)
SoftwareElementState	SMALLINT	SoftwareElementState partly identifies CIM_SoftwareElement (The SoftwareElementState is defined in this model to identify various states of a SoftwareElement life cycle. A SoftwareElement in the deployable state describes the details necessary to successfully distribute it and the details (checks and actions) required to move it to the installable state (for example, the next state). A SoftwareElement in the installable state describes the details necessary to successfully install it and the details (checks and actions) required to create an element in the executable state (for example, the next state). A SoftwareElement in the executable state describes the details necessary to successfully start it and the details (checks and actions) required to move it to the running state for example, the next state). A SoftwareElement in the running state describes the details necessary to manage the started element. CIM_SoftwareElement.SoftwareElementState enumeration 0 = Deployable, 1 = Installable, 2 = Executable, 3 = Running)

Column Name	Data Type	Description
Version	NVARCHAR(64)	Version partly identifies CIM_SoftwareElement; Software Version should be in the form <Major>.<Minor>.<Revision> or <Major>.<Minor><letter><revision>
Name	NVARCHAR(256)	Name partly identifies CIM_SoftwareElement; the name used to identify this software element
TargetOperatingSystem	SMALLINT	TargetOperatingSystem partly identifies CIM_SoftwareElement (The TargetOperatingSystem property specifies the Element operating system environment. The value of this property does not ensure that it is binary executable. Two other pieces of information are needed. First, the version of the operating system must be specified using the class, CIM_OSVersionCheck. The second piece of information is the architecture that the operating system runs on. This information is verified using CIM_ArchitectureCheck. The combination of these constructs clearly identifies the level of operating system required for a particular SoftwareElement. See CIM_OperatingSystem.OSType Enumeration.)
InstallDate	BIGINT	Inherited from CIM_ManagedSystemElement.InstallDate; the datetime value indicating when the object was installed
R_Date	NVARCHAR(256)	A field used by reporting
R_Status	NVARCHAR(256)	A field used by reporting
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; a textual description of an object
DeviceSW_Purpose	SMALLINT	DeviceSoftware_Purpose; an enumerated integer to indicate the role this software plays in regards to its associated Device; CIM_DeviceSoftware.Purpose enumeration (0 = Unknown, 1 = Other, 2 = Driver, 3 = Configuration Software, 4 = Application Software, 5 = Instrumentation, 6 = Firmware, 7 = BIOS, 8 = Boot ROM)
DeviceSW_PurposeDescription	NVARCHAR(512)	A free-form string to provide more information for the DeviceSW Purpose property

Column Name	Data Type	Description
swd_VersionWeight	INT	swd_VersionWeight is of CIM_SoftwareElement; a field used by Software Version Polling
dc_OtherVersionInfo	NVARCHAR(64)	Not standard. A string that specifies the version of this item
R_Type	NVARCHAR(64)	A field used by reporting.

CIM_SoftwareIdentity table

Column Name	Data Type	Description
SoftwareIdentity_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Used to partially identify CIM_SoftwareIdentity
SnapShotID	BIGINT	Used to partially identify CIM_SoftwareIdentity

Column Name	Data Type	Description
InstanceID	NVARCHAR(255)	<p>InstanceID opaquely and uniquely identifies an instance of this class. To ensure uniqueness within the NameSpace, the value of InstanceID SHOULD be constructed using the following 'preferred' algorithm:</p> <p>"<OrgID>:<LocalID> " Where <OrgID> and <LocalID> are separated by a colon ':' and where <OrgID> must include a copyrighted, trademarked, or otherwise unique name that is owned by the business entity creating/defining the InstanceID or is a registered ID that is assigned to the business entity by a recognized global authority. (This is similar to the <Schema Name>_<Class Name> structure of Schema class names.) In addition, to ensure uniqueness <OrgID> must note contain a colon (":"). When using this algorithm, the first colon to appear in InstanceID must appear between <OrgID> and <LocalID>.</p> <p><LocalID> is chosen by the business entity and should not be re-used to identify different underlying (real-world) elements. If the above 'preferred' algorithm is not used, the defining entity must assure that the resultant InstanceID is not re-used across any InstanceIDs produced by this or other providers for this instance's NameSpace. For DMTF defined instances, the preferred algorithm must be used with the <OrgID> set to <i>CIM</i>.</p> <p>An example might be "HEWLETT:PACKARD:HPCPQASM.EXE:7.15.19.0"</p>
VersionString	NVARCHAR(255)	A string representing the complete software version information (Because varying semantics and representations might not allow simple calculation and comparison, both numeric and string representations are provided. See MajorVersion, MinorVersion, RevisionNumber and BuildNumber for the numeric components.)
Manufacturer	NVARCHAR(255)	Manufacturer of this software
Description	NVARCHAR(512)	Description of this element
MajorVersion	SMALLINT	Major version number of this element
MinorVersion	SMALLINT	Minor version number of this element
RevisionNumber	SMALLINT	Revision number of this element
BuildNumber	SMALLINT	Build number of this element

Column Name	Data Type	Description
DeviceSW_Purpose	SMALLINT	An enumerated integer to indicate the role this software plays in regards to its associated Device; CIM_DeviceSoftware.Purpose enumeration (0 = Unknown, 1 = Other, 2 = Driver, 3 = Configuration Software, 4 = Application Software, 5 = Instrumentation, 6 = Firmware, 7 = BIOS, 8 = Boot ROM)
TargetType	NVARCHAR(256)	Key file name.; an application-specific invariant identifier that is consistent between versions of a SoftwareIdentity (It is consistent across more major changes to the Software Identity naming structure. The purpose of the parameter is to allow Software Identities to be selected by a client that are compatible with a specific SoftwareInstallationService. A client uses this parameter to select candidate Software Identities by comparing TargetType with the contents of the SupportedTargetTypes parameter in SoftwareInstallationServiceCapabilities.)
TargetOperatingSystem	SMALLINT	The TargetOperatingSystem property specifies the Element operating system environment (The value of this property does not ensure that it is binary executable. Two other pieces of information are needed. First, the version of the operating system must be specified using the class, CIM_OSVersionCheck. The second piece of information is the architecture on which the operating system runs. This information is verified using CIM_ArchitectureCheck. The combination of these constructs clearly identifies the level of operating system required for a particular SoftwareElement. See CIM_OperatingSystem.OSType Enumeration.)
InstallDate	NVARCHAR(256)	Installation date of this element in CIM date-time format
swd_VersionWeight	INT	swd_VersionWeight is of CIM_SoftwareElement; a field used by Software Status Polling
dc_OtherVersionInfo	NVARCHAR(64)	Not standard; a string that specifies the version of this item
SoftwareElementState	SMALLINT	Used for reporting purposes
Device_SW_PurposeDescription	NVARCHAR(512)	A free-form string to provide more information for the DeviceSW_Purpose property

Column Name	Data Type	Description
R_Type	NVARCHAR(64)	A field used by reporting
R_Date	NVARCHAR(256)	A field used by reporting
R_Status	NVARCHAR(256)	A field used by reporting

CIM_StoragePool table

Column Name	Data Type	Description
StoragePool_LUID	BIGINT	Used to uniquely identify CIM_StorageVolume
NodeID	BIGINT	Used to partially identify CIM_StorageVolume
SnapShotID	BIGINT	Used to partially identify CIM_StorageVolume
ElementName	NVARCHAR(255)	Used for reporting purposes
InstanceID	NVARCHAR(255)	Used for reporting purposes
PoolID	NVARCHAR(255)	Used for reporting purposes
Primordial	BIT	Used for reporting purposes
TotalManagedSpace	BIGINT	Used for reporting purposes
RemainingManagedSpace	BIGINT	Used for reporting purposes

CIM_StorageVolume table

Column Name	Data Type	Description
StorageVolume_LUID	BIGINT	Used to uniquely identify CIM_StorageVolume
NodeID	BIGINT	Used to partially identify CIM_StorageVolume
SnapShotID	BIGINT	Used to partially identify CIM_StorageVolume
DataRedundancy	SMALLINT	Used for reporting purposes
ElementName	NVARCHAR(255)	Used for reporting purposes
NameFormat	SMALLINT	Used for reporting purposes
NoSinglePointOfFailure	BIT	Used for reporting purposes
PackageRedundancy	SMALLINT	Used for reporting purposes
Name	NARCHAR(1024)	A label by which the object is known
SystemCreationClassName	NARCHAR(256)	Used for reporting purposes
SystemName	NARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NARCHAR(256)	Used for reporting purposes
DeviceID	NARCHAR(64)	Used for reporting purposes
Availability	SMALLINT	Used for reporting purposes

Column Name	Data Type	Description
BlockSize	BIGINT	Used for reporting purposes
NumberOfBlocks	BIGINT	Used for reporting purposes
ConsumableBlocks	BIGINT	Used for reporting purposes
IsBasedOnUnderlyingRedundancy	BIT	Used for reporting purposes
SequentialAccess	BIT	Used for reporting purposes
R_OperationalStatus	NARCHAR(256)	Used for reporting purposes
R_ExtentStatus	NARCHAR(256)	Used for reporting purposes
R_RaidLevel	NARCHAR(256)	Used for reporting purposes

CIM_TCPProtocolEndpoint table

Column Name	Data Type	Description
TCPProtocolEndpoint_LUID	BIGINT	Used for reporting purposes
NodeID	BIGINT	Used for reporting purposes
SnapshotID	BIGINT	Used for reporting purposes
Name	NVARCHAR(1024)	A label by which the object is known
SystemCreationClassName	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes
ProtocolIFType	SMALLINT	Used for reporting purposes
PortNumber	NVARCHAR(256)	Used for reporting purposes

Classifications_values table

Column Name	Data Type	Description
ClassificationsId	BIGINT	Used for reporting purposes
ClassificationsValue	SMALLINT	Used for reporting purposes
ClassificationsPos	INT	Used for reporting purposes

ComputerSys_HAP table

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes

ComputerSys_LogicalPortGroup table

Column Name	Data Type	Description
Antecedent	BIGINT	Used for reporting purposes

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes

ComputerSys_NetworkPort table

Column Name	Data Type	Description
GroupComponent	BIGINT	Used for reporting purposes
PartComponent	BIGINT	Used for reporting purposes

ComputerSys_PortController table

Column Name	Data Type	Description
GroupComponent	BIGINT	Used for reporting purposes
PartComponent	BIGINT	Used for reporting purposes

ComputerSys_SAP table

Column Name	Data Type	Description
AvailableSAP	BIGINT	Used for reporting purposes
ManagedElement	BIGINT	Used for reporting purposes

ComputerSys_SCSIProtoCont table

Column Name	Data Type	Description
GroupComponent	BIGINT	Used for reporting purposes
PartComponent	BIGINT	Used for reporting purposes

ComputerSys_SCSIProtoEndp table

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes

ComputerSys_SoftwareIdent table

Column Name	Data Type	Description
System	BIGINT	Used for reporting purposes
InstalledSoftware	BIGINT	Used for reporting purposes

ComputerSys_StorageVol table

Column Name	Data Type	Description
GroupComponent	BIGINT	Used for reporting purposes
PartComponent	BIGINT	Used for reporting purposes

DB_DeviceInfo table

The DB_DeviceInfo table contains general system information. Any system that supports SNMP has information in this table. The DB_DeviceInfo fields are defined in the following table.

Column Name	Data Type	Description
*DeviceKey	INT	
UpdateTime	DATETIME	Date and time the database record was last updated
Description	CHAR (200)	System description.
Location	CHAR (200)	Physical location (must be filled in at the system)
Contact	CHAR (200)	The contact for this system (must be filled in at the system)

Note:



An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

DB_DeviceInfoEx table

The DB_DeviceInfoEx table contains basic information for systems that are running the HP SIM agent or a standard Desktop Management Interface (DMI) service layer. The DB_DeviceInfoEX fields are defined in the following table.

Column Name	Data Type	Description
*DeviceKey	INT	The DeviceKey associates a system with its collected set of data; system information is linked to the device table using the DeviceKey
UpdateTime	DATETIME	Date and time the database record was last updated
TotalMemory	INT	Total amount of system memory
ROMVersion	CHAR (80)	System ROM version
SerialNumber	CHAR (80)	System serial number

Column Name	Data Type	Description
AssetTag	CHAR (100)	System asset tag (must be filled in at the system)
OSName	CHAR (100)	Operating system name. <i>Note:</i> This is not the same OSName from the tool definitions files; this is the OSNameStr value from mxnode
OSType	CHAR(100)	The OSType identifier that is used for tool definitions OSName field; this is a value like WINNT, HPUX, or LINUX
OSVersion	CHAR (100)	Operating system version
OSVendor	CHAR(64)	Vendor name of the operating system
ClusterName	CHAR (100)	If present, the name of the cluster to which this system belongs
OSDescription	CHAR(100)	The description of the host operating system
TrustStatus	Int	System trust state for HP Web enabled agents

Note:



An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

DC_Enclosure table

Column Name	Data Type	Description
Enclosure_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies dc_Enclosure
SnapshotID	BIGINT	Snapshot partly identifies dc_Enclosure
Tag	NVARCHAR(256)	Tag partly identifies dc_Enclosure and is an arbitrary string that uniquely identifies the enclosure and serves as the Element key
dc_Address	INT	The unique address of the enclosure within the rack
dc_EnclosureMaxNumBladesX	INT	The maximum number of server blades the enclosure can contain
dc_EnclosureMaxNumBladesY	INT	The maximum number of server blades the enclosure can contain
dc_FusePresent	NVARCHAR(32)	Specifies if the fuse described is present in the system: Other (1), Absent (2) and Present (3)

Column Name	Data Type	Description
dc_FuseCondition	NVARCHAR(32)	The condition of the fuse (Other (1), Fuse status detection is not supported, OK (2), Fuse is operating properly, Failed (4), Fuse has been tripped or is not operating properly)

DC_ProliantHost table

Column Name	Data Type	Description
ProliantHost_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Identifies the system ID for this row
SnapshotID	BIGINT	Identifies the snapshot ID for this row
dc_SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
dc_SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name where NodeID is equal.
OverallCondition	NVARCHAR(16)	This object represents the overall status of the server host system represented by this MIB
MIBStatusArray	NVARCHAR(512)	An array of MIB status structures (Each structure is made up of 4 octets. The first octet is the MIB presence. The second octet is MIB condition. The third octet is MIB major revision. The fourth octet is MIB minor revision. These blocks of 4 octets each are index by the mib identifier just after the HP enterprise (for example, in 1.3.6.1.232.11 mib, the index is 11). The 4 octets in the first block (block 0) are reserved for systems management and serve as an aggregate of their MIBs.)
GUID	NVARCHAR(64)	The globally unique identifier of this server (If the operating system cannot determine a unique ID, it defaults the variable to contain all 0's. The management station can then perform a SET to this variable to provide the unique ID.)
WebManagementPort	INT	This item indicates the port used by the HP Insight Management Agent
ASRStatus	NVARCHAR(16)	The Automatic Server Recovery (ASR) feature status (If this object is currently Other (1) or Not Available (2), all set operations fail. Any attempt to set this object to Other (1) or Not Available (2) by a management station fails. Setting this object to Disabled (3) or Enabled (4) disables or enables the ASR feature.)

Column Name	Data Type	Description
SystemID	INT	The HP System ID; this value indicates the HP system ID of the system board in this system (This ID replaces the product ID used in older machines (cpqSiProductId). A value of 7Eh for the cpqSiProductId indicates that the cpqSiSystemId should be used to identify the HP system. A value of zero (0) indicates that the system ID function is not supported on this machine. In this case, the cpqSiProductId should be used to identify the system.)
ServerRole	NVARCHAR(64)	The system role; this is a settable free form text field intended to be assigned by a remote console briefly describing the system's function
ServerRoleDetail	NVARCHAR(512)	The system detailed description; this is a settable free form text field intended to be assigned by a remote console describing the system function in detail
ConfigChangeDate	BIGINT	The date and time when the agents were last loaded
SystemUptime	BIGINT	The total time (in minutes) the system has been in full operation (while the server health supporting software was running)

Dedicated_values table

Column Name	Data Type	Description
DedicatedId	BIGINT	Used to uniquely identify this row
DedicatedValue	SMALLINT	Used for reporting purposes
DedicatedPos	INT	Used for reporting purposes

Note:



An asterisk (*) indicates that the field is part of the primary key of the table; where multiple fields in the same table show an asterisk, the primary key connects to each

DeviceNames table

The DeviceNames table contains the names for devices as determined by the various protocols that this device supports. The DeviceNames fields are defined in the following table.

Column Name	Data Type	Description
*DeviceKey	INT	The deviceKey associates a system with its collected set of data (System information is linked to a system using the DeviceKey from the devices table)
nameSNMP	CHAR (60)	The name for this system obtained through SNMP
nameIPX	CHAR (60)	The name for this system obtained through a name service (such as WINS or DNS) or the hosts file
nameDMI	CHAR (60)	The name for this system obtained through DMI
NameFullDNS	CHAR (90)	This is the fully qualified DNS name (if available)
nameActiveDisc	CHAR (60)	This field is no longer an active field

Note:



An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

Device Extended Attributes database table

The Device Extended Attributes fields are defined in the following table.

Column Name	Data Type	Description
snoozeTimeMin	INT	The value in minutes a system will be disabled starting with the time marked by snoozeStartTime
snoozeStartTimeMs	Long	The initial timestamp from when a system was placed in a disabled state

Devices table

The Devices table contains discovered system information. This is the primary table used to define system related data. The Devices fields are defined in the following table.

Column Name	Data Type	Description
DeviceKey	INT	The DeviceKey associates a system with its collected set of data (System information is linked to the device table using the DeviceKey)
Name	CHAR (255)	The name of the system
GUID	CHAR (128)	Globally Unique Identifier, a unique key used to identify this system on the network in the event that it changes its network address (This requires that a system support retrieval of this value in order for it to be stored here.)
Discovered	BIGINT	The date and time that the system was discovered represented as the number of milliseconds since 1970 UTC
ProductType	INT	The product type for this item (See the nodeTypesEnum table, which is best viewed using the deviceSubTypesEnum view, for additional information.)
ProductTypeStr	Char(32)	A string representation of the product type (See the nodeTypesEnum table, which is best viewed using the deviceTypesEnum view, for additional information.)
ProductSubType	CHAR(32)	The subtype, if any (See the NodeSubTypesEnum table, which is best viewed using the deviceSubTypesEnum view, for additional mapping information)
ProductName	CHAR (100)	Product name (such as ProLiant 1500)
OverallStatus	INT	Indicates the overall status of the system (0 = Unknown, 1 = Normal, 2 = Warning, 3 = Minor, 4 = Major, 5 = Critical, 10 = No Status (occurs for new systems or on startup before polling))
LockFlags	INT	Indicates whether product type, name, or both are locked so that discovery cannot change them <ul style="list-style-type: none"> ● 0 = Nothing is locked.
Timestamp	BIGINT	RESERVED (The last time some system information was updated, in the database, not just in this table.)
FullDNSName	VARCHAR (90)	The full DNS name of the system
MxGUID	CHAR(32)	The HP SIM uniquely assigned identifier for this system

DeviceProtocolInfo table

The Device Protocol Information fields are defined in the following table.

Column Name	Data Type	Description
DeviceKey	INT	The DeviceKey associates this table with the system in the devices table.
IPAddressable	INT	Flag indicating if this system is addressable through TCP/IP
IPXAddressable	INT	Flag indicating if this system is addressable through IPX
SNMP	INT	Flag indicating if this system, supports SNMP-based management; a value of -1 indicates the system was not identified yet; a value of 0 indicates SNMP was not found on the system; a value of 1 to 5 indicates that SNMP was found on the system
SNMPverStr	NVARCHAR(32)	A string indicating what version of SNMP was detected (Currently HP Systems Insight Manager only supports "1.0")
HTTP	INT	Flag indicating if this system supports HTTP-based management; a value of -1 indicates the system was not yet identified; a value of 0 indicates HTTP was not found on the system a value of 1 indicates that HTTP was found on the system
DMI	INT	Flag indicating if this system supports DMI-based management; a value of -1 indicates the system was not yet identified; a value of 0 indicates DMI was not found on the system; a value of 1 indicates DMI was found on the system
DMIVerStr	NCHAR(32)	Always 2.0.
WBEM	INT	If WBEM is detected on the system, then this is set to 1; otherwise, it is set to 0
WBEMverStr	NCHAR(32)	The version of WBEM that HP SIM found on the system
SSH	INT	If SSH was detected on the system this is set to 1; otherwise, it is set to 0
SSHverStr	NCHAR(64)	The System ID returned from the SSH request
PrimaryAddress	nchar(32)	For future expansion.
WMIProxyID	INT	The device key of the system that is used for the WMI proxy for the system for this record (In other words HP SIM uses the system with same device key as the WMIProxyID for making WBEM to requests through the WMI Mapper running on that other system.)

ExtentStatus_values table

Column Name	Data Type	Description
ExtentStatusId	BIGINT	Used for reporting purposes
ExtentStatusValue	SMALLINT	Used for reporting purposes
ExtentStatusPos	INT	Used for reporting purposes

DeviceSnmpSettings table

The DeviceSnmpSettings table contains the SNMP settings currently configured for the systems. The DeviceSnmpSettings fields are defined in the following table.

Column Name	Data Type	Description
*DeviceKey	INT	Associates a system with its collected set of data (This system information is linked using the DeviceKey from the devices table.)
networkTimeout	INT	The network timeout value in seconds
networkRetries	INT	The number of retries to be used for SNMP requests
icmpTimeout	INT	ICMP ping timeout value in seconds
icmpRetries	INT	The number of ICMP ping retries to perform
defaultProtoMask	INT	Defines if this system uses defaults (Global protocol settings) for some or all protocols or its individual settings (This is a bitmask field where the different bits define what defaults are to be used. The values are logically ordered together: 1 = use the default SNMP read community, 2 = use the default SNMP write community, 4 = use the default SNMP timeout, 8 = use the default SNMP retries, 16 = use the default icmp timeout, 32 = use the default ICMP retries, 64 = use the default WBEM user name, 128 = use the default WBEM password)

Note:



An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

HP_Cluster table

Column Name	Data Type	Description
HPCluster_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_NParCell
SnapshotID	BIGINT	Snapshot partly identifies HP_NParCell
MembershipIncarnation	BIGINT	An integer value used to uniquely identify the cluster membership (A change in the membership of the cluster results in an increase in the MembershipIncarnation. Thus, a higher value of this property indicates a more recent set of cluster members (found by following the HP_ParticipatingCS associations.)
Name	NVARCHAR(256)	A label by which the object is known
Interconnect	NVARCHAR(256)	A free-form string that describes the interconnection mechanism for the cluster
dc_Types	NVARCHAR(256)	The cluster types (This specifies whether the cluster is for failover (value=2), performance (3), and so on. The values which can be specified are not mutually exclusive. ValueMap { "0", "1", "2", "3", "4", "5", "6" } Values { "Unknown", "Other", "Failover", "Performance", "Distributed OS", "Node Grouping", "SysPlex" })

HP_Node table

Column Name	Data Type	Description
HPNode_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_Node
SnapshotID	BIGINT	Snapshot partly identifies HP_Node
Name	NVARCHAR(256)	A label by which the object is known
Membername	NVARCHAR(256)	Describes the name for this member in the generic HP cluster (The inherited Name value must be fully qualified and unique within the enterprise, while the MemberName value can be an abbreviated version unique within the cluster.)
MemberID	INT	An integer value uniquely identifying this cluster member in the generic HP Cluster; assigned when the system is first added to the cluster and remains unchanged until the system is removed from the cluster (when this instance is deleted) (If the member is re-added later to the cluster, a new instance is created, with a different MemberID value.)

HP_NParCabinet table

Column Name	Data Type	Description
NParCabinet_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_NParCell
SnapshotID	BIGINT	Snapshot partly identifies HP_NParCell
CabinetType	BIGINT	Values are: Unknown(0), Other(1), 8-cell full height cabinet(2), 4-cell full height cabinet(3), 4-cell half-height cabinet(4), 2-cell cabinet(5), I/O expansion cabinet(6). Examples of these cabinet types: 8-cell full height cabinet (SD-32000), 4-cell full-height cabinet (SD-16000), 4-cell half-height cabinet (rp8620), 2-cell cabinet (rx7620)
Label	NVARCHAR(256)	Display string containing the cabinet number, for example <i>cab0</i>
ServiceProcessorCount	NVARCHAR(256)	Number of service processors in this cabinet
ServiceProcessorLocation	NVARCHAR(1024)	Array of long display names for the location of service processors in this cabinet (On cabinets where the service processor is location on a core I/O card, it will include a specification of which card, for example <i>cab0, coreio0</i>)
ServiceProcessorStatus	NVARCHAR(256)	Array of status of any service processors in this cabinet, in the same order as ServiceProcessorLocation; values are: Unknown(0), Other(1), Active(2), Backup(3)

HP_NParCell table

Column Name	Data Type	Description
NParCell_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_NParCell
SnapshotID	BIGINT	Snapshot partly identifies HP_NParCell
SlotID	INT	The ID of the slot the NPar Cell resides in
TotalMemoryInstalled	BIGINT	Total memory (MB) installed in the cell
CPUCount	SMALLINT	The actual number of processors on this cell
CPU Speed	INT	The clock speed in megahertz of the processors on the cell
FirmwareRevision	NVARCHAR(256)	Displayable firmware revision string
DIMMSlotPopulated	NVARCHAR(256)	Array, indexed by DIMM slot number, indicating whether the slot contains a DIMM (Note: This property might not be available when the cell is powered off.)
ConnectedToIOChassis	BIT	True if this cell is connected to an IO chassis

Column Name	Data Type	Description
MaxCPUCount	INT	The maximum number of processors supported on this cell, accounting for both the number of processor module slots and the maximum number of processors per module supported by this platform (The value might not reflect the maximum number of processors in this cell given the number of processor per module actually installed. The maximum number of processors per module supported by this system can be computed by dividing this value by CPUModuleSlotCount.)
CPUSlotPopulated	NVARCHAR(256)	Array, indexed by processor slot number; true when the processor slot is populated (Note that the processor slot number divided by the CPUCountPerModule gives the processor module slot number. All processor slots where that value is equal are in the same processor module.)
CellArchitecture	SMALLINT	The architecture of the processors on this cell; values are Unknown(0), Other(1), PA-RISC(2) and Itanium®-based(3)
ComponentStatus	SMALLINT	Status of this component; values are: Unknown(0), Other(1), Powered Off(2), Powering On(3), Inactive(4), Active(5) (A component is powering on when power has been turned on, but it is still performing power-on self-tests (POST). A component is Inactive if it has completed POST, but has not joined its nPartition. This might be because the component is not assigned to a nPartition, if it is assigned to a nPartition and the nPartition is not active, if the component failed during nPartition boot, if the component was assigned to an active nPartition and no reboot or shut down for reconfiguration of the nPartition has been done, or the component has been configured to remain inactive when the nPartition boots. A component is active when it has joined a nPartition during boot. Note that the status of the component does not imply anything about the state of the operating system on the nPartition. The component will be active, for example, while the operating system is still in the boot process. The status is Unknown if a failure occurred while getting the data for this component.)

Column Name	Data Type	Description
ConnectedIOChasssId	INT	I/O Chassis ID of the chassis to which the cell is connected (The property is not present if ConnectedToIOChassis is false.)

HP_NParComplex table

Column Name	Data Type	Description
NParComplex_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_NParComplex
SnapshotID	BIGINT	Snapshot partly identifies HP_NParComplex
ProfileID	INT	Profile ID of the NPar Complex
dc_ComputeCabCount	INT	Number of compute cabinets in the complex
dc_IOXCabCount	INT	Number of IOX cabinets in the complex
ComplexName	NVARCHAR(256)	Name of the NPar Complex
RevisionString	NVARCHAR(256)	Displayable revision string
MaxPartitionsSupported	SMALLINT	The maximum number of nPartitions that this complex can support (For example, an rp7410 system can support no more than 2 nPartitions.)
CreatorSerialNumber	NVARCHAR(256)	The serial number of the complex as assigned by the original manufacturer
CreatorProductName	NVARCHAR(256)	The name of the product as assigned by the OEM manufacturer (This property is supported only on Itanium®-based platforms but might not be present on all of those.)
OEMSerialNumber	NVARCHAR(256)	The name of the product as assigned by the OEM manufacturer (This property is supported only on Itanium®-based platforms but might not be present on all of those.)
OEMSerialNumber	NVARCHAR(256)	The serial number of the complex as assigned by an OEM manufacturer (This property might not be supported on all platforms.)
OEMProductName	NVARCHAR(256)	The name of the product as assigned by the OEM manufacturer (This property is supported only on Itanium®-based platforms but might not be present on all of those.)
OriginalProductOrderNumber	NVARCHAR(256)	The product order number for this complex as originally delivered, for example, AxxxxxA (If the complex has been upgraded, this is the product order number before the upgrade.)

Column Name	Data Type	Description
CurrentProductOrderNumber	NVARCHAR(256)	The product order number for this complex as it current exists (If the complex has been upgraded, this is the product order number after the upgrade.)
UUID	NVARCHAR(128)	A 16-byte value used for software licensing (This property might not be supported on all platforms.)
CellAssignments	NVARCHAR(256)	Array of values, indexed by cell ID; provides the nPartition ID of the nPartition in to which this cell is assigned or 255 if the cell has type equal to Free, user settable (On iCOD systems, requires iCOD software approval to modify.)

HP_NParIOChassis table

Column Name	Data Type	Description
NParIOChassis_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_NParIOChassis
SnapshotID	BIGINT	Snapshot partly identifies HP_NParIOChassis
ConnectedCellID	INT	ID of the cell
PopulatedPCISlotCount	SMALLINT	Number of occupied PCI slots in this chassis.

HP_NParIOChassisSlot table

Column Name	Data Type	Description
NParIOChassisSlot_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_NParChassisIOSlot
SnapshotID	BIGINT	Snapshot partly identifies HP_NParChassisIOSlot
ID	INT	ID of the NPar I/O Chassis Slot
CabinetID	INT	ID of the cabinet in which the I/O Chassis belongs
IOBayNumber	INT	Bay number in the cabinet where the I/O Chassis resides
Number	INT	The I/O Chassis number that is unique across the bay

HP_NPartition table

Column Name	Data Type	Description
NParPartition_LUID	BIGINT	LUID uniquely defining this table row

Column Name	Data Type	Description
NodeID	BIGINT	Node partly identifies HP_NParPartition
SnapshotID	BIGINT	Snapshot partly identifies HP_NParPartition
PartitionID	INT	ID of the NPar Partition
dc_TotalCPU	INT	Total CPUs in the NPar Partition
dc_InstalledCells	INT	Number of installed cells in the NPar Partition
dc_PoweredOnCells	INT	Number of powered on cells of the NPar Partition
PartitionName	NVARCHAR(256)	Name of the NPar Partition
dc_CoreCell	INT	Core cell Index in the NPar Partition
dc_CoreCellCabinet	INT	Core cell Index in the Cabinet of the NPar Partition
dc_HasInterleaveMem	INT	Flag to indicate if the NPar Partition has Interleave Memory configured (1 = yes)
R_dc_HasInterleaveMemory	NVARCHAR(256)	A field used by reporting
PartitionNameLabel	NVARCHAR(256)	Concatenation of the nPartition name and its label, for example, "MyPartition (par2)"
PartitionType	SMALLINT	Type of cells in this nPartition; values are Unknown(0), Other(1), PA-RISC(2) and Itanium®-based(3)
PartitionsDefined	BOOLEAN	True if this partition currently exists (has been configured in the complex), otherwise false
CoreCellID	INT	The cell ID of the core cell for this nPartition, or 255 if the nPartition is not booted
PrimaryBootPath	NVARCHAR(256)	The primary boot path for this nPartition; present and settable when BootPathsAreAvailable is true, user-settable
AlternateBootPath	NVARCHAR(256)	The alternate boot path for this nPartition; present and settable for all nPartitions on PA-RISC platforms, but is present and settable only for the nPartition on which the provider is running on Itanium®-based platforms, user-settable
HAAlternateBootPath	NVARCHAR(256)	The HA alternate boot path for this nPartition; present and settable when BootPathsAreAvailable is true, user-settable

HPUX_BaseKernelParameter table

Column Name	Data Type	Description
BaseKernelParameter_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_BaseKernelParameter

Column Name	Data Type	Description
SnapshotID	BIGINT	Snapshot partly identifies HPUX_BaseKernelParameter
BaseKernelParameterID	INT	BaseKernelParameterID partly identifies HPUX_BaseKernelParameter. Index of Kernel Configure Group
settingID	NVARCHAR(256)	Name of the kernel configure parameter
CurrentValue	NVARCHAR(256)	Value of the kernel configure parameter

HPUX_Bundle table

Column Name	Data Type	Description
Bundle_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_Bundle
SnapshotID	BIGINT	Snapshot partly identifies HPUX_Bundle
IdentifyingNumber	NVARCHAR(64)	Inherited from CIM_Product.IdentifyingNumber; product identification such as a serial number in software, a die number on a hardware chip, or a project number
Version	NVARCHAR(64)	Inherited from CIM_Product.Version; product version information; corresponds to the Version property in the Product object in the DMTF Solution Exchange Standard
Vendor	NVARCHAR(256)	Inherited from CIM_Product.Vendor; the name of the Product's supplier, or entity selling the Product (the manufacturer, reseller, OEM); corresponds to the Vendor property in the Product object in the DMTF Solution Exchange Standard
Name	NVARCHAR(256)	Inherited from CIM_Product.Name; commonly used product name
Architecture	NVARCHAR(64)	Local to HPUX_Bundle; a vendor-defined string used to distinguish variations of a product (It is used for presentation purposes and for resolving software specifications. If a product with the same value of the Revision and Vendor Tag attributes has different versions of software for different target architectures or any other variation (such as supportedlocale), then the value of the architecture attribute is different for each version. No additional semantics are assumed for its value.)

Column Name	Data Type	Description
Location	NVARCHAR(256)	Location is of HPUX_Bundle; local to HPUX_Bundle; used for resolving software specifications for installed software. A specific product location refers to all filesets of that product that are installed at that location (This is the path beneath which the relocatable files of that product are stored.)
QualifierID	NVARCHAR(64)	Local to HPUX_Bundle; specified by a user when installing software and used for identifying a product (or set of product versions) using a logical name
CreateTime	BIGINT	Local to HPUX_Bundle; a value set by the implementation to be the time that the catalog information for this object was first written; stored as MS since the Epoch
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; the Description property provides a textual description of the object
ModificationTime	BIGINT	Local to HPUX_Bundle; a value set by the implementation to be the time that the catalog information for this object was last written; stored in MS since the Epoch
Size	NVARCHAR(32)	Local to HPUX_Bundle; the sum of the sizes in bytes of all files and control files contained within the software object (For objects other than filesets, the value is computed dynamically as required.)
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; the Caption property is a short textual description of the object
Copyright	NVARCHAR(256)	Local to HPUX_Bundle; the copyright notice for the bundle
Directory	NVARCHAR(256)	Local to HPUX_Bundle; the vendor-defined directory commonly associated with the product (Generally, this is the directory in or below which all (or mostly all) files within the product are installed. For a product that has filesets with the Is Locatable attribute equal to true, all files that contain this directory as the first part of their path can be relocated to the Location Directory during installation by replacing the product.directory portion with the product.location.)

Column Name	Data Type	Description
InstanceIdentifier	NVARCHAR(16)	Local to HPUX_Bundle; a single attribute that distinguishes versions of products (and bundles) with the same Tag (It is a simple form of the version distinguishing attributes, valid only within the context of an exported catalog.)
IsLocatable	bit	Local to HPUX_Bundle; a Boolean value indicating whether any of the filesets in the product have the Is Locatable attribute set to true
LayoutVersion	NVARCHAR(64)	Local to HPUX_Bundle; this attribute and its value, are included for future use
MachineType	NVARCHAR(64)	Local to HPUX_Bundle; a software pattern matching string describing valid machine members of the uname structure as defined by POSIX.1 (2) section 4.4.1 (It is used for determining compatibility.)
SKUNumber	NVARCHAR(64)	Inherited from CIM_Product.SKUNumber; product SKU information
OperatingSystemName	NVARCHAR(256)	Local to HPUX_Bundle; a software pattern matching string describing valid sysname members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)
OperatingSystemRelease	NVARCHAR(256)	Local to HPUX_Bundle a software pattern matching string describing valid release members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)
OperatingSystemVersion	NVARCHAR(64)	Local to HPUX_Bundle; a software pattern matching string describing valid version members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)
ISPatch	bit	Local to HPUX_Bundle; a Boolean value indicating whether this software object is a patch
InstallSource	NVARCHAR(256)	Local to HPUX_Bundle; location of source from where software was installed
DataModelRevision	Nvarchar(64)	Local to HPUX_Bundle; supplies information on version of POSIX compatibility and corresponds to the operating system release that packaged or installed the software
InstallDate	BIGINT	Local to HPUX_Bundle; date timestamp of day, month, year and time when the software was installed on the system; stored as MS since the Epoch

Column Name	Data Type	Description
Contents	NVARCHAR(256)	Local to HPUX_Bundle; the Fileset Software Specification of the bundle's content

HPUX_DNSService table

Column Name	Data Type	Description
DNSService_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_DNSService
SnapshotID	BIGINT	Snapshot partly identifies HPUX_DNSService
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	Equates to CIM_ComputerSystem.Name were NodeID is equal
Name	NVARCHAR(256)	Inherited from CIM_ManagedSystemElement.Name; the Name property defines the label by which the object is known
SearchList	NVARCHAR(512)	The search list for host-name lookup; this attribute and Domain Name attribute are mutually exclusive
Addresses	NVARCHAR(512)	Specifies the IP addresses in dot notation format of the name server that the resolver should search (It can list up to 9 name servers. These names are space delimited.)

HPUX_Fileset table

Column Name	Data Type	Description
Fileset_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_Fileset
SnapshotID	BIGINT	Snapshot partly identifies HPUX_Fileset
SoftwareElementID	BIGINT	Inherited from CIM_SoftwareElement.SoftwareElementID; this is an identifier for the SoftwareElement and is designed to be used in conjunction with other keys to create a unique representation of the element
Name	NVARCHAR(256)	Inherited from CIM_SoftwareElement.Name; the name used to identify this software element
Version	NVARCHAR(64)	Inherited from CIM_SoftwareElement.Version; Software Version should be in the form <Major>.<Minor>.<Revision> or <Major>.<Minor><letter><revision>

Column Name	Data Type	Description
TargetOperatingSystemName	SMALLINT	Inherited from CIM_SoftwareElement.TargetOperatingSystemName (Uses CIM_OperatingSystem.OSType enumeration: 0 = Unknown, 1 = Other, 2 = MACOS, 3 = ATTUNIX, 4 = DGUX, 5 = DECNT, 6 = Digital Unix, 7 = OpenVMS, 8 = HPUX, 9 = AIX, 10 = MVS, 11 = OS400, 12 = OS/2, 13 = JavaVM, 14 = MSDOS, 15 = WIN3x, 16 = WIN95, 17 = WIN98, 18 = WINNT, 19 = WINCE, 20 = NCR3000, 21 = NetWare, 22 = OSF, 23 = DC/OS, 24 = Reliant UNIX, 25 = SCO UnixWare, 26 = SCO OpenServer, 27 = Sequent, 28 = IRIX, 29 = Solaris, 30 = SunOS, 31 = U6000, 32 = ASERIES, 33 = TandemNSK, 34 = TandemNT, 35 = BS2000, 36 = LINUX, 37 = Lynx, 38 = XENIX, 39 = VM/ESA, 40 = Interactive UNIX, 41 = BSDUNIX, 42 = FreeBSD, 43 = NetBSD, 44 = GNU Hurd, 45 = OS9, 46 = MACH Kernel, 47 = Inferno, 48 = QNX, 49 = EPOC, 50 = IxWorks, 51 = VxWorks, 52 = MiNT, 53 = BeOS, 54 = HP MPE, 55 = NextStep, 56 = PalmPilot, 57 = Rhapsody, 58 = Windows 2000, 59 = Dedicated, 60 = OS/390, 61 = VSE, 62 = TPF, 63 = Windows Me, 64 = Caldera Open UNIX, 65 = OpendBSD, 66 = Not Applicable)
CreateTime	BIGINT	A value set by the implementation to be the time that the catalog information for this object was first written.; stored as MS since the Epoch
Description	NVARCHAR(32)	Inherited from CIM_ManagedElement.Description; this property provides a textual description of the object
ModificationTime	BIGINT	A value set by the implementation to be the time that the catalog information for this object was last written; stored as MS since the Epoch
Size	NVARCHAR(32)	The sum of the sizes in bytes of all files and control files contained within the software object (For objects other than filesets, the value is computed dynamically as required.)
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; a short textual description of the object

Column Name	Data Type	Description
ControlDirectory	NVARCHAR(256)	The name of the fileset control directory below which the control files for the fileset are stored within an exported catalog
ISKernel	bit	A boolean value indicating the fileset requires a kernel rebuild
ISLocatable	bit	A boolean value indicating whether the fileset can be relocated during installation
ISReboot	bit	A boolean value indicating the host on which the fileset is configured should be re-booted
Location	NVARCHAR(256)	Specifies the location below which relocatable files are stored (This attribute is only valid for filesets in installed software. It differs from the product.directory attribute only if relocation was specified during installation.)
MediaSequenceNumber	NVARCHAR(256)	A list of values which identify the medium on which the files for this fileset is found
SoftwareElementState	SMALLINT	An enumeration: 0 = Deployable, 1 = Installable, 2 = Executable, 3 = Running
DataModelRevision	NVARCHAR(64)	Supplies information on version of POSIX compatibility and corresponds to the operating system release that packaged or installed the software
InstanceIdentifier	NVARCHAR(16)	A single attribute that distinguishes versions of products (and bundles and filesets) with the same Tag (It is a simple form of the version distinguishing attributes, valid only within the context of an exported catalog.)
InstallDate	BIGINT	Date timestamp of day, month, year and time when the software was installed on the system; stored as MS since the Epoch
Architecture	NVARCHAR(64)	A vendor-defined string used to distinguish variations of a product; used for presentation purposes and for resolving software specifications (If a product with the same value of the Revision and Vendor Tag attributes has different versions of software for different target architectures or any other variation (such as supported locale), then the value of the architecture attribute shall be different for each version. No additional semantics are assumed for its value.)
MachineType	NVARCHAR(64)	A software pattern matching string describing valid machine members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)

Column Name	Data Type	Description
OperatingSystemName	NVARCHAR(64)	A software pattern matching string describing valid sysname members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)
OperatingSystemRelease	NVARCHAR(256)	A software pattern matching string describing valid release members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)
OperatingSystemVersion	NVARCHAR(64)	A software pattern matching string describing valid version members of the uname structure as defined by POSIX.1 (2)Use t section 4.4.1 (It is used for determining compatibility.)
InstallSource	NVARCHAR(128)	Location of source from where software was installed
ISPatch	bit	A Boolean value indicating whether this software object is a patch
ISSparse	bit	Denotes a fileset that is not complete, but one that has been qualified as an update (as opposed to a patch) (One outcome of updating through a sparse fileset is that the catalog information from the old fileset is merged into the new fileset and the old fileset is then removed, leaving the system in the same state as it would be after an update of a full fileset. This option should be used in conjunction with an ancestor attribute showing exactly which versions of software this sparse fileset can update. Filesets that are sparse are only useful when installed along with those versions or when those versions are already installed.)
PatchState	NVARCHAR(16)	Only applied to installed patches; characterizes the current state of an installed patch
AppliedPatches	NVARCHAR(256)	Only applicable to installed patches; specifies the software on which this patch fileset has been applied
SupersededBy	NVARCHAR(256)	Lists what patch superseded this patch
SavedFileDirectory	NVARCHAR(256)	Used by swinstall during the installation of this patch fileset to save the patched files if patch_save_files was set to true at that time (When rolling back or committing this patch, this attribute is used to determine the directory to access those saved files.)

HPUX_HFS table

Column Name	Data Type	Description
HFS_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	
SnapshotID	BIGINT	
Name	NVARCHAR(256)	Inherited from CIM_FileSystem.Name; the inherited Name serves as key of a FileSystem instance within a ComputerSystem
CreationClassName	NVARCHAR(256)	Equates to HPUX_HFS
CSCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
CSName	NVARCHAR(256)	Equates to CIM_ComputerSystem.Name where NodeID is equal
Root	NVARCHAR(256)	Inherited from CIM_FileSystem.Root; path name or other information defining the root of the FileSystem
ReadOnly	bit	Inherited from CIM_FileSystem.ReadOnly; indicates that the FileSystem is designated as read only
FileSystemType	NVARCHAR(256)	Inherited from CIM_FileSystem.FileSystemType; string describing the type of FileSystem and its conventions (For example, \"NTFS\" or \"S5\" can be as well as any additional information on the FileSystem implementation. Because various flavors of FileSystems (like S5) exist, this property is defined as a string.)
FileSystemSize	BIGINT	Inherited from CIM_FileSystem.FileSystemSize; the total size of the File System in bytes (If unknown, enter 0.)
BlockSize	BIGINT	Inherited from CIM_FileSystem.BlockSize.The FileSystem's block size for data storage and retrieval
AvailableSpace	BIGINT	Inherited from CIM_FileSystem.AvailableSpace; the total amount of free space for the FileSystem, in bytes
RemoteFileSystem_Name	NVARCHAR(256)	Inherited from CIM_ManagedSystemElement.Name; a label by which an object is known
Freelnodes	BIGINT	Inherited from CIM_UnixLocalFileSystem.FreeInodes; the number of free inodes present in the file system

Column Name	Data Type	Description
TotalNodes	BIGINT	Inherited from CIM_UnixLocalFileSystem.TotalNodes; the total number of inodes available in the file system. 0 indicates this file system does not have a preset limit
FSReservedCapacity	BIGINT	Inherited from CIM_UnixLocalFileSystem.FSReservedCapacity; the reserve data capacity of the file system in bytes
Bootable	bit	Indicates whether a file system is a bootable
LargeFileSupported	bit	Indicates that this file system supports large files
MinimumFreespace	bit	Indicates the minimum percentage of free disk spaces allowed
FragmentSize	INT	Specifies the fragment block size of this file system
InodeSize	INT	Specifies the density of Inodes in this file system
SectorsPerTrack	INT	The number of sectors per track on the disk
TracksPerCylinder	INT	Specifies the number of tracks per cylinder on the disk
DiskCylindersPerCylinderGroup	INT	Specifies the number of disk cylinders per cylinder group
DiskRevolutionsPerSecond	INT	Specifies the number of disk revolutions per second
RotationalDelay	INT	Specifies the expected time in MS to service a transfer completion interrupt and initiate a new transfer on the same disk
dc_MountedFileSystems	INT	The total number of currently mounted file systems

HPUX_LogicalVolume table

Column Name	Data Type	Description
LogicalVolume_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_LogicalVolume
SnapshotID	BIGINT	Snapshot partly identifies HPUX_LogicalVolume
Name	NVARCHAR(256)	Name of Logical Volume in the System
DeviceID	NVARCHAR(64)	Inherited from CIM_LogicalDevice.DeviceID; an address or other identifying information to uniquely name the Logical Device

Column Name	Data Type	Description
Access	SMALLINT	Inherited from CIM_StorageExtent.Access; describes whether the media is readable, writeable, or both (An enumeration: 0 = Unknown, 1 = Readable, 2 = Writeable, 3 = Read/Write Supported, 4 = Write Once)
LogicalExtentSize	BIGINT	Computed by multiplying HPUX_LogicalVolume.BlockSize by HPUX_LogicalVolume.NumberOfBlocks
Capacity	BIGINT	Capacity of logical volume in number of logical extent
MirrorCopyNumber	INT	Number of the mirrored Copy for the logical volume
ConsistencyRecovery	NVARCHAR(64)	Consistency Recovery Method for the mirrored logical volume. No value for NOT mirrored Logical Volume (MWC, NOMWC, NONE)
SchedulePolicy	NVARCHAR(64)	Access Scheduling Policy of the logical volume; might have values such as (Striped, Sequential, Parallel)
NumberOfStripes	INT	Number of stripes for the logical volume
StripeSize	INT	Size of stripes for logical volume; value in KB
BadBlockRelocation	BIT	Switch of Bad Block Relocation feature; true if it is on, false otherwise
AllocationPolicy	NVARCHAR(64)	Allocation Policy of the logical volume; might contain values such as (Non-Strict, Non-Strict/Contiguous, Strict, Strict/Contiguous, PVG-Strict, PVG-Strict/Contiguous, PVG-Strict/Distributed, Unknown)
StaledLogicalExtent	INT	Counter of staled Logical Extent in the logical volume; valid only the logical volume is mirrored
NumberReadAccesses	INT	Number of read accesses to the logical volume
NumberWriteAccesses	INT	Number of write accesses to the logical volume
Status	NVARCHAR(64)	Availability status of Logical Volume; might contain values such as (Available/State, Available/Syncd, Available, Unavailable)

HPUX_NISServerService table

Column Name	Data Type	Description
NISServerService_LUID	BIGINT	LUID uniquely defining this table row

Column Name	Data Type	Description
NodeID	BIGINT	Node partly identifies HPUX_NISServerService
SnapshotID	BIGINT	Snapshot partly identifies HPUX_NISServerService
Name	NVARCHAR(256)	Inherited from CIM_ManagedSystemElement.Name; the Name property defines the label by which the object is known
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	Equates to CIM_ComputerSystem.Name where NodeID is equal
CreationClassName	NVARCHAR(256)	Equates to HPUX_NISServerService
ServerWaitFlag	SMALLINT	The NIS Server Wait Flag; makes the host wait for a response for the NIS server (An enumeration: 0 = Unknown, 1 = Other, 2 = Wait, 3 = No Wait)
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; a short textual description of the object
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; provides a textual description of the object
ServerType	SMALLINT	Returns what type of NIS Server the managed system is; if the system is not a NIS server, returns None (An enumeration: 0 = Unknown, 1 = Other, 2 = None, 3 = NIS Master, 4 = NIS Slave)

HPUX_NTPService table

Column Name	Data Type	Description
NTPService_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_NTPService
SnapshotID	BIGINT	Snapshot partly identifies HPUX_NTPService
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	Equates to the value of CIM_ComputerSystem.Name where NodeID is equal
CreationClassName	NVARCHAR(256)	Equates to HPUX_NTPService
Name	NVARCHAR(256)	Inherited from CIM_ManagedSystemElement.Name; the Name property defines the label by which the object is known

Column Name	Data Type	Description
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; a short textual description of the object
ServerAddress	NVARCHAR(512)	This attribute is specified by hostname that appears in the file <code>/etc/hosts</code> , or it is an IP Address in dot notation format (Multiple servers are specified as comma delimited names.)
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; provides a textual description of the object

HPUX_PhysicalVolume table

Column Name	Data Type	Description
PhysicalVolume_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_PhysicalVolume
SnapshotID	BIGINT	Partly identifies HPUX_PhysicalVolume
Name	NVARCHAR(256)	Name of Physical Volume in the System
DeviceID	NVARCHAR(64)	Inherited from CIM_LogicalDevice.DeviceID; an address or other identifying information to uniquely name the LogicalDevice (Might return the name of the physical volume. For example, <code>/dev/dsk/c0t0d0</code> .)
AlternatePVName	NVARCHAR(256)	Can return alternate physical volume path name (For example, <code>/dev/rdisk/c0t0d0</code> ; returns the same as DeviceID replacing "dsk" for "rdsk")
Status	NVARCHAR(32)	Availability status of Physical Volume. Returns (Available; Unavailable).
PhysicalExtentSize	BIGINT	Size in bytes; calculated by multiplying HPUX_PhysicalVolume.BlockSize by the HPUX_PhysicalVolume.NumberOfBlocks
Capacity	BIGINT	Capacity of the whole Physical Volume in number of Physical Extent
Allocated	INT	Size of the allocated Physical Volume in number of Physical Extent
Free	INT	Size of the free Physical Volume space in number of Physical Extent
NumberStaledPEs	INT	Counter of Staled Physical Extent in the Physical Volume

HPUX_Product table

Column Name	Data Type	Description
Product_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_Product
SnapshotID	BIGINT	Snapshot partly identifies HPUX_Product
IdentifyingNumber	NVARCHAR(64)	Inherited from CIM_Product.IdentifyingNumber; product identification such as a serial number on software, a die number on a hardware chip, or a project number
Name	NVARCHAR(256)	Inherited from CIM_Product.Name; commonly used Product name
Version	NVARCHAR(64)	Inherited from CIM_Product.Version; a vendor-defined string describing the revision of the product
Vendor	NVARCHAR(256)	Inherited from CIM_Product.Vendor; the name of the product supplier or entity selling the product (the manufacturer, reseller, or OEM)
Architecture	NVARCHAR(64)	A vendor-defined string used to distinguish variations of a product (It is used for presentation purposes and for resolving software specifications. If a product with the same value of the revision and Vendor Tag attributes has different versions of software for different target architectures or any other variation (such as supported locale), then the value of the architecture attribute is different for each version. No additional semantics are assumed for its value.)
Location	NVARCHAR(256)	Used for resolving software specifications for installed software (A specific product location refers to all filesets of that product that are installed at that location. This is the path beneath which the relocatable files of that product are stored.)
QualifierID	NVARCHAR(64)	Specified by a user when installing software and used for identifying a product (or set of product versions) using a logical name
CreateTime	BIGINT	A value set by the implementation to be the time that the catalog information for this object was first written; stored as MS since the Epoch
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; the Description property provides a textual description of the object

Column Name	Data Type	Description
ModificationTime	BIGINT	A value set by the implementation to be the time that the catalog information for this object was last written; stored as MS since the Epoch
Size	NVARCHAR(32)	The sum of the sizes in bytes of all files and control files contained within the software object (For objects other than filesets, the value is computed dynamically as required.)
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; is a short textual description of the object
AllFileSets	NVARCHAR(256)	Contains the actual filesets that make up a product (This is a list of all filesets defined for the product, as opposed to what is currently installed, described by the filesets attribute. The all_filesets attribute is used to determine completeness of this product when another software object has a dependency on this product. In checking a product prerequisite or corequisite, the existence of a fileset.tag in all_filesets that is not actually installed or available indicates that the dependency is not satisfied. This does not affect exerequisites because they test whether any of the contents of the dependency specification are present instead of all of the contents tested for prerequisites or corequisites.)
ControlDirectory	NVARCHAR(256)	The name of the product control directory below which the control files for the product are stored within an exported catalog
Copyright	NVARCHAR(256)	The copyright notice for the product
Directory	NVARCHAR(256)	The vendor-defined directory commonly associated with the product (Generally, this will be the directory in or below that all (or mostly all) files within the product are installed. For a product which has filesets with the Is Locatable attribute equal to true, all files which contain this directory as the first part of their path can be relocated to the Location Directory during installation by replacing the product.directory portion with the product.location.)
InstanceIdentifier	NVARCHAR(16)	A single attribute that distinguishes versions of products (and bundles) with the same Tag (It is a simple form of the version distinguishing attributes, valid only within the context of an exported catalog.)

Column Name	Data Type	Description
ISLocatable	bit	A boolean value indicating whether any of the filesets in the product have the Is Locatable attribute set to true
PostKernelPath	NVARCHAR(256)	The path to the script that is run after the kernel filesets have been installed. Any product containing kernel filesets should include this path (If this attribute is supplied, the corresponding script is executed if it exists relative to the root directory of the installed software. If this attribute is not supplied, then the implementation defined path (the default value for the attribute) is used if it exists relative to the root directory of the installed software. Note that the use of an alternative root directory might mean that the default path does not exist relative to the root directory of the installed software.)
LayoutVersion	NVARCHAR(64)	This attribute and its value, are included for future use
MachineType	NVARCHAR(64)	A software pattern matching string describing valid machine members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)
SKUNumber	NVARCHAR(64)	The semantics associated with the values of this attribute are undefined; can be used to store such vendor-defined values as part number, order number, or serial number
OperatingSystemName	NVARCHAR(256)	A software pattern matching string describing valid sysname members of the uname structure as defined by POSIX.1 (2), section 4.4.1; used for determining compatibility
OperatingSystemRelease	NVARCHAR(256)	A software pattern matching string describing valid release members of the uname structure as defined by POSIX.1 (2), section 4.4.1; used for determining compatibility
OperatingSystemVersion	NVARCHAR(64)	A software pattern matching string describing valid version members of the uname structure as defined by POSIX.1 (2), section 4.4.1; used for determining compatibility
ISPatch	bit)	A Boolean value indicating whether this software object is a patch
InstallSource	NVARCHAR(128)	Location of source from where software was installed

Column Name	Data Type	Description
DataModelRevision	NVARCHAR(8)	Supplies information on version of POSIX compatibility and corresponds to the operating system release that packaged or installed the software
InstallDate	BIGINT	Date timestamp of day, month, year and time when the software was installed on the system; stored as MS since the Epoch

HPUX_VolumeGroup table

Column Name	Data Type	Description
VolumeGroup_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_VolumeGroup
SnapshotID	BIGINT	Snapshot partly identifies HPUX_VolumeGroup
CollectionID	NVARCHAR(64)	Inherited from CIM_DiskGroup.CollectionID; the identification of the Collection object
Name	NVARCHAR(256)	Name of Volume Group in the System
AccessPermission	NVARCHAR(64)	Access Permission of Volume Group in the System; can be one of the following (Read-Only; Read-Write)
Status	NVARCHAR(32)	Availability status of Volume Group in the System; can be one of the following values (Available; Unavailable)
PhysicalExtentSize	INT	The size of the fundamental physical extent size in bytes
Capacity	INT	Capacity of whole Volume Group in number of Physical Extent
Allocated	INT	Allocated space in the volume group in number of Physical Extent
FreeSpace	INT	Number of free Physical Extents in the volume group
MaxNumberOfPVs	INT	Max number of definable physical volume in the volume group
NumberOfDefinedPVs	INT	Number of max allocatable Physical Extent from physical volume
NumberOfActivePVs	INT	Number of current defined physical volume in the volume group
MaxNumberOfLVs	INT	Max number of definable logical volume in the volume group
NumberOfDefinedLVs	INT	Number of current defined logical volume in the volume group
NumberOfActiveLVs	INT	Number of current active logical volume in the volume group

Column Name	Data Type	Description
NumberOfPVGroups	INT	Total number of physical volume group in this volume group

IPAddress table

The IPAddress table contains the known IP addresses for the devices. The IPAddress fields are defined in the following table.

Column Name	Data Type	Description
*DeviceKey	INT	Associates a system, with its collected set of data; system information is linked to the device table using the DeviceKey
*ipindex	INT	The addresses index for the system, for example, 0 is the first IP address. 1 is the second and and so on
*IPAddress	CHAR (16)	TCP/IP address (x.x.x.x)
IPAddressNumber	bigint	A numeric representation of the IP address
MACaddr	CHAR (12)	The MAC address of the system network card (without and delimiter, such as ":" or "-")
IPsubnetMask	CHAR (16)	The TCP/IP subnet mask (x.x.x.x)
IFtype	IFtype	The interface type

Note:



An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

IPProtocolEnd_NetworkPort table

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes

Note:



An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

IPXAddress table

The IPXAddress table contains the known IPX addresses for the systems. The IPXAddress fields are defined in the following table.

Column Name	Data Type	Description
*DeviceKey	INT	Associates a system with its collected set of data; system information is linked to the devices table using the DeviceKe
*IpxIndex	INT	A unique IPX index for the system used mainly when 2 or more IPX addresses exist for a system
*IPXAddress	CHAR (25)	IPX address for this system

Note:



An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

OperationalStatus_SVvalues table

Column Name	Data Type	Description
OperationalStatusId	BIGINT	Used for reporting purposes
OperationalStatusValue	BIGINT	Used for reporting purposes

PhysicalPackage_Product table

Column Name	Data Type	Description
PartComponent	BIGINT	Used for reporting purposes
GroupComponent	BIGINT	Used for reporting purposes

SCSIProtoCont_SCSIProtoEnd table

Column Name	Data Type	Description
AvailableSAP	BIGINT	Used for reporting purposes
MangedElement	BIGINT	Used for reporting purposes

SCSIProtocolCont_SoftwareId table

Column Name	Data Type	Description
System	BIGINT	Used for reporting purposes
InstalledSoftware	BIGINT	Used for reporting purposes

SCSIProtoEnd_SCSIProtoEnd table

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes

NetworkAddresses_values table

Column Name	Data Type	Description
NetworkAddressesId	BIGINT	Uniquely identifies this row
NetworkAddressesValue	NVARCHAR(64)	Used for reporting purposes
NetworkAddressesPos	INT	Used for reporting purposes

NodeSnapshot table

Column Name	Data Type	Description
Snapshot_LUID	BIGINT	Snapshot partly identifies NodeSnapshot
NodeID	BIGINT	Node partly identifies NodeSnapshot
Tag	NVARCHAR(256)	Contains the user-defined tag
Description	NVARCHAR(512)	Description of the user-defined tag
CollectionDateTime	BIGINT	Stored as MS since the Epoch
DetailedInformation	NVARCHAR(512)	Additional collection status information
ReturnCode	SMALLINT	Binary status information. Zero indicates no error
Status	NVARCHAR(256)	Status of the snapshot for the system; used by different reports
DataAvailable	INT	Currently unused, reserved
FilterID	BIGINT	Currently unused, reserved for collection filter ID

NodeTypesEnum table

Column Name	Data Type	Description
enumOrd	INT	The enumeration identifier for this entry (This can be used when linking in the deviceTypesEnum view. This should also match the productType value in the devices table.)
enumLabel	char(64)	Unique (non displayable) string used for identifying a product type (This is the only value guaranteed to be unique across any installation.)

NodeSubTypesEnum table

Column Name	Data Type	Description
enumOrd	INT	The enumeration identifier for this entry (This can be used when linking in the deviceSubTypesEnum view.)
enumLabel	char(64)	This is a unique (non displayable) string used for identifying a product subtype (This is the only value guaranteed to be unique across any installation. This can be linked to the devices tables productSubType field.)

Notices table

The Notices table contains all the events received or generated, such as Discovered Device events, SNMP traps and so on. The Notices fields are defined in the following table.

Column Name	Data Type	Description
*NoticeId	INT	Unique identifier for this notice instance
State	INT	<ul style="list-style-type: none"> ● 1=In Progress ● 2=Not Cleared (active) ● 5=Cleared
NoticeType	INT	Index into the noticeType table
NoticeSeverity	INT	1 = Normal, 2 = Warning, 3 = Minor, 4 = Major, 5 = Critical, 100 = Informational
NoticePriority	INT	RESERVED
DeviceKey	INT	Index into the devices table
Generated	bigint	Date/time notice was generated or received represented as the number of milliseconds since 1970 UTC
Cleared	bigint	Date/time notice was cleared represented as the number of milliseconds since 1970 UTC
Completed	bigint	RESERVED
LastChecked	bigint	RESERVED
LastModified	bigint	Date/time notice was cleared represented as the number of milliseconds since 1970 UTC
JobID	char(128)	If this notice is related to some job, this is the job ID for that job
Timestamp	bigint	RESERVED
AssignedTo	VARCHAR (255)	User names to which an event is assigned
Comments	VARCHAR(1000)	User input comments for one or more events

Note:

An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

NoticeType table

The NoticeType table defines all of the event types that can be processed. The NoticeType fields are defined in the following table.

Column Name	Data Type	Description
*NoticeType	INT	System assigned identifier.
GUID	Char(32)	Unique system assigned identifier
TypeIdStr	CHAR (255)	A unique String Identification for the event
dispHandler	CHAR (255)	Internal handler for the display of the event
rxHandler	Char(255)	Internal handler for event reception, usually blank.
defaultSeverity	Int	A default severity to use for the event
Privilege	Int	The internal privilege level a user must have to view the event details
ServiceEnable	INT	Used when the CRSM is installed
ServiceEnable	INT	Used when the CRSM is installed
ProviderID	INT	Used when the CRSM is installed

Note:

An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

OperationalStatus_CSvalues table

Column Name	Data Type	Description
OperationalStatusId	BIGINT	Used for reporting purposes
OperationalStatusValue	SMALLINT	Used for reporting purposes
OperationalStatusPos	INT	Used for reporting purposes

OperationalStatus_NPvalues table

Column Name	Data Type	Description
OperationalStatusId	BIGINT	Used for reporting purposes
OperationalStatusValue	SMALLINT	Used for reporting purposes
OperationalStatusPos	INT	Used for reporting purposes

operationalStatus_PCvalues table

Column Name	Data Type	Description
OperationalStatusId	BIGINT	Used for reporting purposes
OperationalStatusValue	SMALLINT	Used for reporting purposes
OperationalStatusPos	INT	Used for reporting purposes

Snapshot table

Column Name	Data Type	Description
SnapshotID	BIGINT	LUID uniquely defining the snapshot
OverallStatus	NVARCHAR(256)	OverallStatus of the Snapshot: Code indicating if the snapshot was successful
SnapshotTag	NVARCHAR(256)	Contains the user-defined tag
CollectionDateTime	BIGINT	Stored as MS since the Epoch

SPAllocatedFromStoragePool table

Column Name	Data Type	Description
SPAllocFromStoragePool_LUID	BIGINT	LUID uniquely defining the SPAllocFromStoragePool
NodeID	BIGINT	Used for reporting purposes
SnapshotID	BIGINT	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes
SpaceConsumed	BIGINT	Used for reporting purposes

SVAllocatedFromStoragePool table

Column Name	Data Type	Description
SVAllocFromStoragePool_LUID	BIGINT	LUID uniquely defining the SVAllocFromStoragePool
NodeID	BIGINT	Used for reporting purposes
SnapshotID	BIGINT	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes
SpaceConsumed	BIGINT	Used for reporting purposes

TCPProtoEnd_IPProtoEnd table

Column Name	Data Type	Description
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes

Windows Event Log

Windows NT/2000 Events

HP Systems Insight Manager (HP SIM) can write the following events to the NT Event Log during normal operation.

Event ID	Event Type
1	Error
2	Warning
3	Informational

Windows NT/2000 Event Log Error Messages

Message	Description
HP SIM error: NNNN StartServiceCtrlDispatcher failed	An attempt was made to start the HP SIM service with an invalid cmdline argument.
HP SIM error: NNNN SetServiceStatus failed	An error was returned when attempting to acquire status from HP SIM.
HP SIM Application Stopped Abnormally	The HP SIM application has performed an abnormal termination.
SNMP and Snptrap services required by HP SIM are not installed or not running	The HP SIM service program has detected that SNMP services are not installed or not running and, thus, will not make an attempt to start the HP SIM application. The service program will automatically terminate.
Failed to set SQL Server 'show advanced options' to 1	HP SIM could not configure the database server.
Failed to set SQL Server 'min server memory' to MemorySizeHere MB	HP SIM could not configure the database server.
The SQL Server 'min server memory' is set to MemorySizeHere MB, which is less than the recommended MemorySizeHere MB	HP SIM configured database server memory usage as specified by user.

Message	Description
Failed to set SQL Server 'show advanced options' back to 0	HP SIM could not configure database server.
NoticeDescriptionHere	HP SIM received a security notice.
Modified SQL Server 'min server memory' from 0 to MemorySizeHere MB	HP SIM configured database server memory usage as specified by user.
Attempting to Restart HP SIM Application	The Auto-restart feature of the HP SIM service program is making an attempt to restart the HP SIM application.
HP SIM Application Started	The HP SIM application has been started by the HP SIM service program.
HP SIM Application Stopped	The HP SIM application has performed a normal termination.
HP SIM Application stopped Abnormally	The HP SIM application has performed an abnormal termination.
HP SIM Installation Complete	The HP SIM program has been successfully created and installation of HP SIM is complete.
HP SIM Service Removed	The HP SIM service program has been successfully stopped and removed.
HP SIM Service Started	The HP SIM service program has successfully started.
HP SIM Service Stopped	The HP SIM service program has successfully terminated.
CPU Cluster Monitor Resource	Connectivity problems exist or definable thresholds for CPU utilization have been exceeded.
Disk Cluster Monitor Resource	Connectivity problems exist or definable thresholds for disk capacity have been exceeded.
System Cluster Monitor Resource	Connectivity problems for receiving system information exist.
SNMP and SNMP trap services required by HP SIM are not installed or not running	The HP SIM service program has detected that SNMP services are not installed or not running and, thus, will not make an attempt to start the HP SIM application. The service program will then terminate normally.
DCOM was unable to communicate with computer<system> using any of the configured protocols	Disable logging the WMI errors. Refer to "WMI Mapper Proxy" for more information.

Service and Support

Service and Support

Support for HP Systems Insight Manager (HP SIM) is provided as an adjunct to support of the underlying hardware. The purpose of the HP Support page is to provide you with a variety of product, service, and support related resources. In particular, you can use this page to:

- Access <http://www.hp.com/servers/manage>. This website is devoted to systems management products. You will find a wealth of product and service related information on this portal.
- Access the links to HP support home page and World Wide Web locator for phone numbers, online tools, and information.
- Contact the HP Support Forum to get answers to your questions about HP products. The HP Support Forum can be found at <http://forums.itrc.hp.com/>.

Keeping good records of your configuration can significantly speed up the troubleshooting process. Consult the following list when you obtain assistance from your HP service provider:

- Management server make, model, and serial number information
- Operating system information, including version number, a list of all service packs that have been applied, the Compaq SSD version, and Insight Agent names and versions that have been applied
- Hardware configuration information:
 - Survey Utility output or Inspect printout
 - System Configuration Utility printout
 - Description of any third-party equipment that is not shown on the Inspect or System Configuration printout

glossary

A

agent	A program that regularly gathers information or performs some other service without the user's immediate presence. HP Systems Insight Manager (HP SIM) agents provide in-depth hardware and software information and subsystem status to HP SIM and numerous third-party management applications. See Also management agent.
alarm	A user-configurable notification displayed in the System Status panel of HP SIM when certain events occur. For instance, if a monitored item changes, an alarm notifies the user that a change has occurred. See Also trap, event.
all events	Systems where any event types have occurred.
All Tools toolbox	A default toolbox that provides complete access to all tools for the authorized system or system group.
attribute	A single characteristic of a manageable product or component, as in an attribute of a Management Information Format (MIF) file. A set of related attributes constitutes a group. For example, the clock speed of a processor chip is an attribute of a group that describes that chip. See Also Management Information Format.
authentication	The process of identifying an individual, based on a user name and password. Authentication is distinct from authorizations and ensures that the individual is who they claim to be.
authorizations	A mapping of a relationship between a user, a toolbox, and a system or system group.
automatic discovery	The process that HP SIM uses to find and identify the systems on your network and populate the database with that information. A system must first be discovered to collect data and track system health status.
available software	A listing of the software components available in the repository to which the VCA has been configured to point. When browsing directly into a VCA, these additional components can be selected for installation.

B

banner	The section of the GUI at the top of the screen that includes the user name and links to the Home page and sign out functions.
--------	---

C

caution	A note to indicate that failure to follow directions could result in damage to equipment or loss of information.
central management server (CMS)	A system in the management domain that executes the HP SIM software. All central operations within HP SIM are initiated from this system.
central processing unit polling rate	The rate for how often the Cluster Monitor CPU Resource checks CPU utilization as reported by HP Insight Management Agent on monitored systems.
certificate	An electronic document that contains a subject's public key and identifying information about the subject. The certificate is signed by a certificate authority (CA) to bind the key and subject identification together. See Also certificate authority.
certificate authority (CA)	A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual who has been granted the unique certificate is the individual they claim to be.
cleared status	A status condition that indicates a system is cleared.
clearing events	Changing the event status from uncleared to cleared.
clients	HP desktop, portable, and workstation systems.
cluster	A parallel or distributed computing system made up of many discrete systems that form a single, unified computing resource. Clusters vary in their features, complexity, and the purposes for which they are best suited.
cluster IP address	The IP address of the cluster.
cluster monitor	A core component of HP SIM. Cluster Monitor adds the ability to monitor and manage multi-node clusters. Cluster Monitor also manages multiple cluster platforms in a heterogeneous environment.
cluster monitor resource	A program that provides a monitoring or management function for clustered nodes in a cluster.
cluster system identification	Information about cluster systems. This information is stored in the database.
collections	The method for grouping system or event searches.
command line interface (CLI)	A program interface where commands can be executed directly from the command shell of the operating system command shell.

common information model (CIM)	An object-oriented schema defined by the Desktop Management Task Force (DMTF). CIM is an information model guide that describes and shares management information enterprise-wide. CIM is designed for extending each management environment in which it is used.
common information model object manager (CIMOM)	A CIMOM acts as the interface for communication between web-based enterprise management (WBEM) providers and management applications such as HP Systems Insight Manager. A CIMOM that provides an interface for an SMI-S provider is called an SMI CIMOM.
communications protocol	See management protocol.
component	A component is a single, self-describing, installable (interactive or silent) binary file containing a single piece of software, such as firmware image, driver, agent, or utility, that is supported by the management and update tools.
configuration history report	The Survey Utility that contains reports that show configuration details for server and compares configuration history files for differences.
Configure or Repair Agents	An HP SIM plug-in feature that enables you to repair credentials for SNMP settings and trust relationships that exist between HP SIM and target systems. You can also update Web Agent passwords on target systems that have 7.1 agents or earlier installed.
control tasks	Sequences of instructions that are associated with a search, event, or both, such as Delete Events, Remove Disk Thresholds, Set Disk Threshold, and Set Device Access community strings.
critical status	A state generated when HP SIM can no longer communicate to a managed system.
custom commands	Tasks that launch an application on the server that is running HP SIM.

D

data collection reports	Data collection reports include information about discovered systems in a single instance or a historical trend analysis report. HP SIM supports Overwrite existing data set (for detailed analysis) , formerly known as Single Instance Data Collection task in Insight Manager 7, and Append new data set (for historical trend analysis) , formerly known as Historical Data Collection task in Insight Manager 7. With Overwrite existing data set (for detailed analysis) , data is collected from a system at a single instance. With Append new data set (for historical trend analysis) , data detailing the system history is collected.
data collection tasks	Procedure that involves gathering information from a group of managed systems and storing that information in the database.

	HP SIM uses Hardware Status Polling and Data Collection Tasks to implement collection.
Desktop Management Interface (DMI)	An industry-standard protocol, primarily used in client management, established by the DMTF. DMI provides an efficient means of reporting client system problems. DMI-compliant computers can send status information to a central management system over a network.
Desktop Management Taskforce (DMTF)	An industry standard body that defines DMI and WBEM standards for the industry. HP is an active sponsor and participant in the DMTF body.
digital signatures	A technology used to validate the sender of a transaction. This technology uses private keys to digitally sign the data and public keys to verify the sender.
discovery	A feature within a management application that finds and identifies network objects. In HP management applications, discovery finds and identifies all the HP systems within a specified network range.
discovery filters	Enables users with full-configuration-rights to prevent or allow certain system types from ever being added to the database.
discovery template	Files that can be used by automatic discovery in lieu of typing the addresses directly in to the Ping inclusion ranges or Exclusion ranges fields on the Automatic Discovery - General Settings page and are designed to be used as a quick way to change the scope of automatic discovery.
Distributed Component Object Model (DCOM)	An extension of the Component Object Model (COM) that enables COM components to communicate between clients and servers on the same network.
distributed task facility (DTF)	A management application that manages the remote execution of tasks on managed systems.
DMI	See Desktop Management Interface.
Domain Name Service (DNS)	A service that translates domain names into IP addresses.

E

e-mail notification	One of the notification tasks in HP SIM that sends notifications through e-mail.
edit collection	To modify existing collections to add or remove search criteria.
enclosure	A physical container for a set of blades servers. It consists of a backplane that routes power and communication signals and additional hardware for cabling and thermal issues. It also hosts the CPU or server power supplies.

event	<p>Information sent to certain users that something in the managed environment has changed. Events are generated from SNMP traps and are preconfigured in this release. HP SIM receives a trap when an important event occurs. Events are defined as:</p> <ul style="list-style-type: none">● Warning. Events of this type indicate a state that might become a problem.● Informational. Events of this type require no attention and are provided as useful information.● Normal. Events of this type indicate that this event is not a problem.● Minor. Events of this type indicate a warning condition that can escalate into a more serious problem.● Major. Events of this type indicate an impending failure.● Critical. Events of this type indicate a failure and signal the need for immediate attention.
event overview	A chart that summarizes the uncleared events by product type.
external sites	Third-party application URLs.

F

full-configuration-rights user	A user who is automatically authorized for the All Tools toolbox on all systems, including the CMS. This type of user has been given special privileges to administer the HP SIM software.
--------------------------------	---

G

graphical user interface (GUI)	A program interface that takes advantage of the graphics capabilities of the computer to make the program easier to use. The HP SIM GUI is Web-enabled and displays in a Web browser.
--------------------------------	---

H

hosts files	A file that includes all critical system information from the HP SIM database, such as IP addresses.
HP Insight Management Agent	A program that regularly gathers information or performs some other service without the user's immediate presence.
HP ProLiant Essentials Virtual Machine Management Pack (VMM)	Provides central management and control of Virtual Machines on Microsoft Virtual server, Vmware's GSX and ESX. Integrated with HP SIM, VMM provides unified management of HP ProLiant host servers and Virtual Machines.
HP ProLiant Essentials Vulnerability and Patch Management Pack	The all-in-one vulnerability assessment and patch management tool integrated into HP SIM, simplifying and consolidating the proactive identification and resolution of issues that can impact server availability into one central console.

HP Systems Insight Manager	<p>System management software that is capable of managing a wide variety of systems, including HP systems, clusters, desktops, workstations, and portables.</p> <p>HP SIM; combines the strengths of Insight Manager 7, HP Tootools, and HP Servicecontrol Manager to deliver a single tool for managing HP ProLiant, Integrity, and HP 9000 systems running Windows, Linux, and HP-UX. The core HP SIM software delivers the essential capabilities required to manage all HP server platforms. HP SIM can also be extended to deliver unparalleled breadth of system management with plug-ins for HP storage, power, client, and printer products. Plug-ins for rapid deployment, performance management, and workload management enable systems administrators to pick the value added software required to deliver complete lifecycle management of their hardware assets.</p>
HP Systems Insight Manager database (database)	The database that stores vital information about HP SIM, including users, systems, and toolboxes.
HP Version Control Agent (VCA)	An agent that is installed on a server to enable you to see the HP software installed on that server. The VCA can be configured to point to a VCRM agent, enabling easy version comparison and software update from the repository.
HP Version Control Repository Manager (VCRM)	An HP agent that enables a customer to manage HP provided software stored in a user-defined repository.
HyperText Transfer Protocol (HTTP)	The underlying protocol used by the World Wide Web.
I	
identification	An aspect of the discovery process that identifies the management protocol and type of system.
installed version	A particular HP software component that is installed on the server the VCA is installed on.
Instant Support Enterprise Edition (ISEE)	Provides proactive remote monitoring, diagnostics, and troubleshooting to help you enhance the availability of HP-UX, Microsoft Windows, Linux, OpenVMS, Tru64 Unix, NonStop, and Sun Solaris servers, as well as storage and network systems in your data center.
Internet Protocol (IP)	Specifies the format of datagrams (packets) and the addressing scheme on a network. Most networks combine IP with Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.
Internetwork Packet Exchange (IPX)	A networking protocol used by the Novell NetWare operating systems and is a datagram (packet) protocol used for connectionless communications.
IP range	Systems with an IP address that falls in the specified range.

J

Java database connectivity (JDBC)	Similar to ODBC, this set of application program interfaces (APIs) provides a standard mechanism to allow Java applets access to a database.
Java Remote Method Invocation (RMI)	A set of protocols that enable Java objects to communicate remotely with other Java objects.

K

key	A value used alone or with an encryption decoder (corresponding public or private key) for cryptography. In traditional private key cryptography, the communicators share a key or cipher so that each can encrypt and decrypt messages. The risk in this system is that if any party loses the key, the system is broken. In public key cryptography, the private key is associated with a public key, so each person in the system has a personal private key that is never shared.
keystore	A database that maintains a list of keys. The keystore can contain a subject's own private key. A keystore can also contain a list of public keys, as published in certificates. See Also key.

L

limited-configuration-rights user	A user who has limited capability to configure the CMS. Limited-configuration-rights users have permission to create, modify, and delete all reports and their own tools.
-----------------------------------	---

M

Major status	Aggregate status information collected from the system that indicates one or more of the monitored subsystems are not operating properly which is impacting the system. Action should be taken immediately.
managed systems	Any system managed by HP SIM, such as servers, desktops, and Remote Insight Boards (RIBs).
management agent	A daemon or process running on a managed system. It receives and executes requests from the CMS on the managed system.
management domain	A collection of resources called managed systems that have been placed under the control of the HP SIM. Each central management server is responsible for a management domain. The managed systems can belong to more than one management domain.
Management HTTP Server	An integrated piece of software used by the HP suite of HP Web-enabled System Management Software to communicate

	over HTTP and HTTPS. It provides a uniform set of functionality and security to HP Web-enabled System Management Software. This version is available in the ProLiant Support Pack 7.10 or earlier.
Management Information Base (MIB)	The data specification for passing information using the SNMP protocol. An MIB is also a database of managed objects accessed by network management protocols.
Management Information Format (MIF)	An ASCII text file in the DMI architecture that describes the manageable features and attributes of a product. The DMI maintains this information in a MIF database and makes it available to operating systems and management applications. The DMTF has specified MIF formats for a variety of system types and peripheral systems.
management instrumentation	Agents running on systems that provide management information for HTTP, DMI, or SNMP protocols.
management LAN	A LAN dedicated to the communications necessary for managing systems. It is typically a moderate bandwidth (10/100 BaseT) and secured through limited access.
management protocol	A set of protocols, such as WBEM, HTTP, SNMP, or DMI, used to establish communication with discovered systems.
management scope	A set of systems within the set of all discovered systems that HP SIM manages.
management services	The provider of a core set of capabilities such as auto-discovery, data collection, a central repository for system and event information, event management, basic notification, and secure access. These functions are used by add-ins from HP, a Management Solutions Partner, and HP SIM users.
management tasks	Procedures you set up to search systems or events.
manual discovery techniques	Processes that enable you to bypass a full discovery for the following tasks: <ul style="list-style-type: none">● Adding a single system● Editing the system● Creating or importing an HP SIM database hosts file● Creating or importing generic hosts files
Microsoft Clustering Service status page	A page that summarizes cluster status as defined by Microsoft Cluster Server and lists the status and values of MSCS-defined cluster attributes. The Cluster Monitor uses color to display status based on MSCS condition values (Normal, Degraded, Failed, and Other).
Minor status	Aggregate status information collected from the system that indicates one or more of the monitored subsystems are not operating properly which is impacting the system. Action should be taken as soon as possible to prevent further failure.

Monitor Tools toolbox A default toolbox that contains tools that display the state of managed systems but not tools that change the state of managed systems.

multiple-system aware (MSA) A run type that supports multi-system operations. Tools with this run type operate on the target systems using their own internal mechanisms instead of using the distributed task facility. The MSA run type uses the distributed task facility to launch the tool on a single system before the tool interacting with the other managed systems.

N

no configuration rights user A user who cannot configure the CMS. However, the user can view and run predefined reports on the CMS and all managed systems.

O

Open Service Event Manager (OSEM) Enables you to collect, filter, and send problem reports for supported systems (ProLiant and Integrity) running Insight Management Agents. In addition, OSEM automatically sends service event notifications to HP SIM when a problem is detected on the system.

overall software status This section indicates whether the software on the server that the VCA is installed on has any updates available within the repository in which it has been configured to monitor.

P

HP ProLiant and Integrity Support Pack An ProLiant and Integrity Support Pack is a set of HP software components that have been bundled together by HP, and verified to work with a particular operating system. An ProLiant and Integrity Support Pack contains driver components, agent components, and application and utility components. All of these are verified to install together.

Performance Management Pack (PMP) A software solution that detects, analyzes, and explains hardware bottlenecks on HP ProLiant servers. PMP tools consist of Online Analysis, Offline Analysis, Comma Separated Value (CSV) File Generator Report, System Summary Report, Status Analysis Report, Configuration, Licensing, and Manual Log Purge.

ProLiant Essentials license key The contractual permissions granted by HP to the customer in the form of a coded embodiment of a license that represents a specific instance of a license. A single license can be represented by a single key or by a collection of keys.

ProLiant Support Pack A set of HP software components that have been bundled together by HP and verified to work with a particular operating system. A ProLiant Support Pack contains driver components, agent

components, and application and utility components. All of these are verified to install together.

R

racks	A set of components cabled together to communicate between themselves. A rack is a container for an enclosure.
Red Hat Package Manager (RPM)	The Red Hat Package Manager is a powerful package manager that can be used to build, install, query, verify, update, and uninstall individual software packages. A package consists of an archive of files and package information, including name, version, and description.
Reference Support Pack	A baseline bundle of HP software components that the VCA can be configured to point to in the repository. This setting enables users to indicate that they want to keep all of their software up to a certain Support Pack level.
remote wakeup	<p>Sometimes referred to as Wake-On-LAN (WOL). The remote powering up of a system through its resident WOL network card, provided that the system has been enabled to be so awakened using the ROM or F10 Setup.</p> <p>This is a capability on which HP SIM relies to turn on the systems for scheduled Software Updates or Replicate Agent Settings.</p>
remove all disk thresholds	A task provided by HP SIM to remove disk thresholds for systems in an associated collection. This task only removes disk thresholds that were set by HP SIM or by browsing directly to the Web agent. Any thresholds set by HP SIM for Windows 32, including disk thresholds, are not removed by this task.
Replicate Agent Settings	A tool that can be used to copy Web-based agent settings to a group of systems.
repository	A directory containing ProLiant Support Pack or Integrity Support Packs and Smart Components.
Resource Partition	<p>A subset of the resources owned by an operating system instance. The use of those resources is controlled through technologies such as the Fair Share Scheduler, pSets, and Memory Resource Groups.</p> <p>A resource partition also has a set of processes associated with it, and only those processes can use the resources within the resource partition. Policies established by tools such as Process Resource Manager (PRM), Workload Manager (WLM), or Global Workload Manager (gWLM) control how resources are allocated to the set of resource partitions within an operating system instance.</p>
role	See toolbox.

rule set Conditions, policies, or criteria applied to system information to determine what it is.

S

search criteria A set of variables (information) used to define a requested subset of information from the set of all information. The information set that can be filtered includes action information, some of the system information, and so on. A filter is composed of an inclusion filter followed by an exclusion filter. The result of these two filtering operations is called a group. An example of a filter is an SQL statement that creates viewable information or causes management operations to be performed.

Secure HTTP (HTTPS) An extension to the HTTP protocol that supports sending data securely over the Web.

Secure Shell (SSH) A program to log in to another system over a network and execute commands on that system. It also enables you to move files from one system to another, and it provides authentication and secure communications over insecure channels.

Secure Sockets Layer (SSL) A standard protocol layer that lies between HTTP and TCP and provides privacy and message integrity between a client and server. A common usage of SSL is to provide authentication of the server, so clients can be assured they are communicating with the server it claims to be. It is application protocol independent.

Secure Task Execution (STE) A feature of HP SIM that securely executes a task from a managed system. STE ensures that the user requesting the task has the appropriate rights to perform the task, and encrypts the request to protect data from snooping.

security roles A feature that enables administrators to restrict system access and manage access on a per-user or per-group basis. This capability enables systems administrators to delegate tasks to junior staff without providing access to advanced or dangerous features. It also enables systems administrators to delegate management of systems to specific organizations or customers without providing access to systems owned by other organizations or customers.

self-signed certificate A certificate that is its own Certificate Authority (CA), such that the subject and the CA are the same.
See Also certificate, certificate authority.

server blade Typically a very dense server system containing microprocessors, memory, and network connections that can be easily inserted into a rack-mountable enclosure to share power supplies, fans, switches, and other components with other server blades. Server blades tend to be more cost-efficient, easier to deploy, and easier to adapt to growth and change than traditional rack-mounted or tower servers.
See Also enclosure, racks.

server blade visual locator	<p>A feature designed to provide visual representation of ProLiant BL e-Class and p-Class servers within their respective enclosures and racks.</p> <p>See Also enclosure, racks.</p>
Service Advertising Protocol (SAP)	<p>A NetWare protocol used to identify the services and addresses of servers attached to the network.</p>
set disk thresholds	<p>A task provided by HP SIM to set a disk threshold for systems in an associated collection. This threshold is set on all disk volumes on the target system.</p>
Shared Resource Domain (SRD)	<p>A collection of compartments—all of the same type—that share system resources. The compartments can be nPartitions, virtual partitions, processor sets (pSets), or Fair Share Scheduler (FSS) groups. A server containing nPartitions can be an SRD—as long as nPartition requirements are met. A server or an nPartition divided into virtual partitions can be an SRD for its virtual partition compartments. Similarly, a server, an nPartition, or a virtual partition containing pSets can be an SRD for its pset compartments. Lastly, a Server, an nPartition, or a virtual partition containing FSS groups can be an SRD for its FSS group compartments.</p> <p>A complex with nPartitions can hold multiple SRDs. For example, if the complex is divided into nPartitions, named Par1 and Par2, Par1's compartments could be virtual partitions, while Par2's compartments are pSets.</p> <p>Each compartment holds a workload. gWLM manages the workload by adjusting the compartment's resource allocation.</p>
Short Message Service (SMS)	<p>A convenient way to send brief text messages directly to a wireless phone. There is a maximum message length of 140 characters.</p>
Simple Network Management Protocol (SNMP)	<p>One of the management protocols supported by HP SIM. Traditional management protocol used extensively by networking systems and most servers. MIB-2 is the standard information available consistently across all vendors.</p>
Single Login	<p>Permission granted to an authenticated user browsing to HP SIM to browse to any of the managed systems from within HP SIM without re-authenticating to the managed system. HP SIM is the initial point of authentication, and browsing to another managed system must be from within HP SIM.</p>
single-system aware (SSA)	<p>A run type that does not support multi-system operations. Tools with this run type are only aware of the system on which they are running.</p>
SMI CIMOM	<p>See common information model object manager.</p>
SMI-S provider	<p>An industry-standard WBEM provider that implements a well defined interface for storage management. The manufacturers of host bus adapters (HBAs), switches, tape libraries, and storage</p>

	arrays can integrate SMI-S providers with their systems, or provide them as separate software packages. See Also Web-Based Enterprise Management.
SNMP communication setting	Default SNMP community string used when communicating with systems supporting SNMP communications.
SNMP trap	Asynchronous event generated by an SNMP agent that the system uses to communicate a fault.
software inventory	A listing of the HP software installed on the system where the VCA is installed.
software update	A task to remotely update software and firmware.
spoofing	The act of a website posing as another site to gather confidential or sensitive information, alter data transactions, or present false or misleading data.
standard error (stderr)	The default place where the system writes error messages. The default is the terminal display.
standard output (stdout)	The default place to which a program writes its output. The default is the terminal display.
status message list	A list created by Cluster Management Resources to collect entries found in the bottom left area of the Cluster Monitor page to bring your attention to cluster attributes that are in an abnormal state.
status message summary header	The list header summary of the total number of status messages in the list and, in parentheses, the number of status messages that have not been examined.
status type	The classification of status messages (for example, Critical, Major, Minor, Normal, Warning, and Unknown).
Storage Management Initiative Specification (SMI-S)	A standard management interface developed by the Storage Networking Industry Association (SNIA). SMI-S provides a common interface and facilitates the management of storage devices from multiple vendors. SMI-S uses industry-standard common information model and Web-Based Enterprise Management technology.
storage systems	SAN-attached Fibre Channel disk arrays, switches, tape libraries, or hosts (with Fibre Channel host bus adapters).
subnet	On TCP/IP networks, subnets are all systems whose IP addresses have the same prefix. For example, all systems with IP addresses that start with 10.10.10. would be part of the same subnet.
Survey Utility	An agent (or online service tool) that gathers and delivers hardware and operating system configuration information. This information is gathered while the server is online.

symmetric key	A common key that both the server and receiver of a message share and use to encrypt and decrypt a message.
system	Systems on the network that communicate through TCP/IP or IPX. To manage a system, some type of management protocol (for example, SNMP, DMI, or WBEM) must be present on the system. Examples of systems include servers, workstations, desktops, portables, routers, switches, hubs, and gateways.
system default searches	Requests for data about aggregate system health status, proactive subsystem status, and detailed component information on servers, workstations, desktops, and portables, irrespective of management protocol.
system group	A group of systems based on a system collection; a static snapshot of the source collection at the time the system group was created. Used for authorizations.
system health status	<p>This is the overall status gathered from protocols (DMI, SNMP, WBEM, Insight Management Agents, and so on) that are supported on a target system. Status is defined as:</p> <ul style="list-style-type: none">● Critical. HP SIM can no longer communicate with the system. The system was previously discovered but cannot be pinged. The system might be down, powered off, or no longer accessible on the network because of network problems.● Major. A major problem exists with this system. It should be addressed immediately. For systems running an HP Insight Management Agent, some component has failed. The system might no longer be properly functioning, and data loss can occur.● Minor. A minor problem exists with this system. For systems running Insight Management Agent, some component has failed but the system is still functioning.● Warning. The system has a potential problem or is in a state that might become a problem.● Normal. The system is functioning correctly.● Disabled. The system is disabled from monitoring but is not necessarily turned off.● Unknown. HP SIM cannot obtain management information about the system.● Informational. The system might be in a transitional or non-error state.
system identification	<p>Identifying information about systems. This information is stored in the database. The following information is identified:</p> <ul style="list-style-type: none">● Type of management protocol on the system (SNMP, DMI, WBEM, HTTP, and SSH)● Type of HP system (server, client, switch, router, and so on)● Network name of system

system information	<p>Information that is provided on the System Page under the Identity tab. The system information includes:</p> <ul style="list-style-type: none">● Network address● Network name● Description● Contact● Location● System links
system information using DMI	Agents that conform to the DMI V2 standard and have passed testing. The list of compliant DMI V2 agents can be found on http://www.dmtf.org .
system information using SNMP	Agents that conform to SNMP MIB-2 standards.
system links	A summary information page for a specific system that has a management agent.
System Management Homepage (SMH)	An integrated piece of software used by the HP suite of HP Web-enabled System Management Software to communicate over HTTP and HTTPS. It provides a uniform set of functionality and security to HP Web-enabled System Management Software.
system overview report	A report indicating the state of systems that is available at the time that HP SIM is first opened. A system search result contains the number of systems that are registered with the HP SIM databases. Systems are grouped by their status conditions. Each number in a column is a hyperlink to a more detailed list of systems, which displays the systems that correspond to the number in the overview.
system search	Logical grouping of systems into a collection based on information in the HP SIM database. After a search is defined, you can display the results from the system view page or associate it with a management task.
system search results	The result of a system search.
system status panel	The section of the GUI on the left of the screen that displays status information and system or event alarms.
system type	One of 12 supplied types. You can add your own based on one of these types. For example, use Server type to create MyServer type. It is still a server and is reported on in the same way, but it has your designation.
System Type Manager (STM)	A utility that enables you to modify the default behavior of discovery and identification of objects classified as Unknown or as another category of systems are discovered and identified precisely as you require. HP SIM discovers and identifies the system and applies the new information when an Unknown system matches a rule set that you specify as the primary rule set.

Furthermore, creating the new system type provides a **System Link** page for viewing the information returned from the system agent or from the communication protocol of SNMP or DMI.

T

task	An executed instance of an HP SIM tool, on one or more systems or systems groups, with a specific set of arguments.
task scheduling	A master scheduling tool for the scheduling of polling, control, and notification tasks.
threshold	A preset limit that produces an event when the limit is reached or exceeded.
timed event	An action that schedules necessary events. Examples of events include backups, disk storage cleanup, and so on. The user defines the tools in this category.
Tomcat	An open source implementation of Java Servlet and JavaServer Pages technologies that is used by HP SIM as a Web server.
tool	An application, command, or script that can be executed by HP SIM on one or more systems to perform a task.
tool category	An organizational structure for grouping tools. A tool must belong to one and only one category. Tool categories can only contain tools. They cannot contain other tool categories.
toolbox	A defined set of tools that a user might need for a particular task, such as database administration or software management. Each HP SIM toolbox is associated with a set of tools.
trap	An unsolicited message generated by a management agent that indicates that an event has occurred. For example, a monitored item has exceeded a set threshold or changed status. Previously called alarm. See Also event.
trap categories	Event collection systems found by event type. SNMP traps categorized by HP SIM into logical groups according to their functions.
trap forwarding address	The IP address of a system that has been specified to receive trap notifications forwarded by the HP SIM systems.
type	The classification of a system, which identifies it as a standard system type. The system types are client, cluster, portable, printer, remote access device, repeater, router, server, switch, unknown, workstation, and other.

U

uncleared event status	<p>Events that have a Critical, Major, Minor, Normal, or Informational severity.</p> <ul style="list-style-type: none"> ● Critical. A failure has occurred, and immediate attention is required. ● Major. A failure is impending. ● Minor. A warning condition exists that can escalate into a more serious problem. ● Normal. These events are not a problem. ● Informational. No attention required. This status is provided as useful information
unknown status	HP SIM cannot obtain management information about the system using SNMP or DMI. Although no management instrumentation information is available, the system can be pinged. It might have an invalid community string or security setting.
user	A network user with a valid login on the CMS that has been added to HP SIM.
user accounts	Accounts used to sign into HP SIM. These accounts associate a local Windows user account or a domain account with privilege levels and paging attributes inside HP SIM.
user configuration page	A page in HP SIM that provides the ability to create and define users that have access to the management application and associated rights.
user group	A group of users defined on the CMS operating system that has been added to HP SIM. Members of the user group in the operating system can sign into HP SIM.

V

VCA log	A listing of all the software maintenance tasks completed by the VCA and reports resulting from those tasks.
version control	Referred to as the VCRM installed on a Windows system for Windows and Linux ProLiant systems, and Software Distributor on HP-UX operating systems. Provides an overview of the software status for all managed ProLiant or Integrity systems and can update system software and firmware on those systems programmatically using predetermined criteria. Version control identifies systems that are running out-of-date system software, indicates if an upgrade is available, and provides reasons for upgrading. For HP-UX systems, Software Distributor can be launched from an HP SIM CMS against one or more installed HP-UX systems.
Virtual Server Environment (VSE)	An integrated server virtualization offering for HP-UX, Linux, and Windows servers that provides a flexible computing environment

maximizing usage of server resources. VSE consists of a pool of dynamically sizeable virtual servers; each can grow and shrink based on service level objectives and business priorities. For more information, go to <http://hp.com/go/vse>.

W

WBEM Services	HP WBEM Services for HP-UX is an HP product that uses WBEM and DMTF standards to manage HP-UX system resources.
Web-Based Enterprise Management (WBEM)	An Industry initiative to provide management of systems, networks, users, and applications across multiple vendor environments. WBEM simplifies system management, providing better access to both software and hardware data that is readable by WBEM compliant applications.
Web-Based Enterprise Services (WEBES)	A tool suite that is aimed at preventing or reducing the downtime of a system.
Web-launch aware (WLA)	A run type for tools that are launched in a Web browser using a Web server. WLA tools can be designed to deal with multiple systems.
Windows Management Instrumentation (WMI)	An API in the Windows operating system that enables systems in a network, typically enterprise networks, to be managed and controlled.
workspace	The section of the GUI where tools are displayed.

X

X client	An application or tool that appears on an X server. X clients can also be called X applications.
X server	A local application that accepts X client requests and acts on them.
X Window System	A cross-platform windowing system that uses the client/server model to distribute services across a network. It enables applications or tools to run on a remote computer.
XML document	A collection of data represented in XML.

Index

Symbols

, 261

A

about, 420, 422

 default polling tasks, 270

 license keys, 339

 login, 143

 searches, 235

 single login, 143

 storage solutions (SNMP), 261, 264

 System License Information Reporting, 350

 trust relationships, 168

 version control agent, 419

accessing, 424–425

 automatic event handling, 506

 discovery filters, 85

 Event Monitoring Service, 454

 HP Array Configuration Utility, 466

 HP BladeSystem Integrated Manager in HP Systems

 Insight Manager, 468

 HP Client Manager, 468

 HP OpenView Storage Data Protector, 460

 HP OpenView Storage Management Appliance,
 462

 HP OpenView Storage Operations Manager, 463

 HP ProLiant Essentials Performance Management
 Pack, 373

 HP Serviceguard Manager, 458

 HP Storage Essentials, 470

 HP StorageWorks Command View EVA, 472

 HP StorageWorks Command View SDM, 471

 HP StorageWorks Command View TL, 472

 HP StorageWorks Command View XP, 471

 HP StorageWorks Command View XP Advanced
 Edition, 471

 HP StorageWorks Modular Smart Array 1000, 473

 HP Web Jetadmin, 470

 Ignite-UX, 456

 Integrated Lights-Out, 456

 Partition Manager, 457

 PMP, 567

 PRM, 463

 property pages, 442

 replicate agent settings, 375

 RPM tools, 378

 SMP, 380–381

 System Fault Management, 443

 System Management Homepage, 382

 VMM, 437

 VPM, 469

 VSE, 469

 WBEM Providers for Linux, 444

 Webmin, 459

adding

 DMI rules, 111

 hosts files to database, 95

 individual keys, 348

 keys from file, 347

 SMP license, 380

 SNMP rules, 111

 STM rule, 103

 systems, 89

 systems to database, 91

 WMI Mapper proxy, 544–545

administering

 events, 504, 506, 508

 software, 502

 user groups, 115

 users, 115

 WMI Mapper proxy, 544

administration

 adding user groups, 119

 authorizations, 114

 authorizations overview, 132

 cluster resource settings, 292

 creating authorization, 133

 creating toolbox, 128

 creating users, 117

 deleting authorizations, 138

 deleting toolboxes, 130

 deleting user groups, 124

 deleting users, 124

 node resource settings, 292

 overview, 502

 report authorizations, 139

 toolboxes overview, 127

 updating authorization, 136

 users overview, 115

 version control repository, 566

administrator-template, 126

agents, 568

alarm, 56

all scheduled tasks, 276, 280, 558

 task results list, 269

 viewing, 281

antivirus software, 601

application

 launching, 326

applying

 time filters, 277, 286, 510, 514, 533, 538

Array Configuration Utility, 446

assistance, 44

- attributes
 - cluster monitor, 296
- audit log, 148, 306, 597
 - configuring, 599
 - viewing, 597
- authentication, 36, 601
- authentication problems, 601
- authorization
 - users, 142
- authorizations, 132, 140
 - adding user groups, 119
 - creating, 132–133
 - creating toolbox, 128
 - creating users, 117
 - delete authorizations, 138
 - deleting, 132, 138
 - deleting toolboxes, 130
 - deleting user groups, 124
 - deleting users, 124
 - editing toolboxes, 129
 - editing user groups, 121
 - editing users, 121
 - overview, 114, 132
 - printing report, 132
 - reports, 139
 - toolbox report, 131
 - updating, 132, 136
 - user group report, 125
 - user report, 125
 - users, 52, 115
 - viewing report, 132
- automatic
 - discovery, 78
- automatic discovery, 36, 52, 76, 79, 85–87, 101, 210, 232, 547–548
 - configuring, 84
- automatic event handling, 36, 50, 52
 - accessing, 506
 - creating new task, 506
 - creating task, 508
 - e-mail settings, 506, 520
 - managing tasks, 506
 - modem settings, 506, 521
- automatic event handling problems, 601
- automatic event handling task
 - creating, 514, 538
 - with existing collection, 514
 - with specific event, 538
 - with specified attributes, 510
- automatic event handling tasks, 504
 - copying, 509
 - creating, 504, 509–510
 - deleting, 504, 509
 - disabling, 509, 519
 - e-mail settings, 504
 - editing, 509
 - enabling, 509, 519
 - managing, 504, 509
 - modem settings, 504
 - task results, 509
 - viewing definition, 509
- B**
 - backup
 - database, 591
 - database for HP-UX, 592
 - database for Linux, 592
 - database for Windows, 592
 - banner, 53
 - basic search, 236
 - bdf, 306
 - bi-weekly data collection, 555
 - blade, 36, 81, 84, 192, 204, 206, 223, 428, 644
 - browser problems, 601
 - browsing
 - CMS, 46
- C**
 - capacity
 - storage arrays, 259
 - cat, 306
 - categories
 - system, 178
 - central management server, 36, 301, 601
 - browsing to, 46
 - overview, 43
 - setting language, 58
 - setting locale, 58
 - setting up trust relationship, 46
 - certificate, 601
 - trusted, 601
 - certificate problems, 601
 - Certificate Signing Request
 - creating, 156
 - importing, 158
 - submitting, 157
 - certificates, 150–153, 155–158, 160, 164–167
 - server, 142, 150
 - setting trust relationships, 168
 - cim_ip.dat, 95
 - CIMOM, 601
 - clear events task
 - running, 522
 - scheduling, 522
 - clearing
 - events, 227, 504, 522, 535
 - CLI, 601

- CLI problems, 601
- client management software, 446
- cluster, 81, 101, 601
 - HP Serviceguard, 216, 458
 - identification, 541
 - identity tab, 399
 - searching, 234
- cluster collections, 291
 - creating, 181
 - customizing, 180–181, 215
 - deleting, 184
 - editing, 183
 - managing, 215
 - overview, 175
 - printing, 215, 221
 - report, 221
 - setting properties, 185
- cluster management, 446
- cluster monitor, 291, 293–295
 - attributes, 296
 - cluster resource settings, 292
 - cluster tab, 293
 - CPU polling rate, 298
 - Disk polling rate, 298
 - MSCS polling rate, 298
 - network tab, 294
 - node resource settings, 292
 - nodes tab, 294
 - polling rates, 298
 - resources, 296
 - resources tab, 295
 - system status polling rate, 298
 - viewing CPU utilization, 298
- cluster monitor resource
 - configure node settings, 292
 - configure settings, 292
 - CPU, 298
 - CPU polling rate, 292
 - CPU thresholds, 292
 - Disk polling rate, 292
 - Disk thresholds, 292
 - MSCS polling rate, 292
 - overview, 296
 - thresholds, 300
- cluster problems, 601
- cluster search results
 - printing, 244
- cluster table view
 - printing results, 216
- cluster table view page, 291
 - adding columns, 220
 - customizing, 216, 220
 - deleting columns, 220
 - navigating, 216
 - overview, 215
 - printing, 221
 - sorting, 220
- clusters, 76
 - deleting, 215, 220
 - deleting from search, 243
 - monitoring, 174
 - MSCS, 291, 293
 - searching, 242
 - Serviceguard Manager, 36
- CMS (see central management server)
- collecting
 - license keys, 338, 341
- collections, 140, 601
 - cluster, 175
 - deleting, 184
 - event, 174–175, 535, 537
 - naming conventions, 254
 - private, 175
 - problems, 601
 - saving, 179, 535
 - shared, 175, 249
 - storage systems, 255, 257
 - system, 174–175
- command line
 - interface, 36, 62
- command line tools, 288, 300–301
 - creating, 302
 - parameters, 325
- Command View
 - discovery, 264
- commands
 - , 62
 - bdf, 300
 - cat, 300
 - cp, 300
 - df, 300
 - find, 300
 - ls, 300
 - mv, 300
 - ps, 300
 - rm, 300
- common tasks, 66
 - Setting up managed systems, 66
- community strings, 70, 210, 548
- comparing snapshots, 499
- compiling
 - Compiling and customizing SNMP MIBs with HP SIM, 66
 - MIB, 364
- complex, 36, 81
 - identity tab, 400
- configuration rights, 114
- configuring

- audit log, 597, 599
- automatic discovery, 84
- Configuring or Repairing Agents, 66
- DML access, 288, 334
- e-mail settings, 52, 520
- event filters, 523
- events, 526
- first time wizard, 50
- HP SIM, 50
- HP Version Control Repository Manager, 566
- iLO, 350
- login events, 148
- modem settings, 521
- pager settings, 52
- PAM on HP-UX, 143
- Pluggable Authentication Modules, 143
- PMP, 567
- protocol settings, 52
- protocols, 550–551
- SNMP access, 288, 335
- SNMP traps, 524
- SSH bypass properties, 596
- storage system discovery, 256
- system link, 148
- timeout options, 149
- tool definition files, 597
- contacting
 - support, 44
- containers
 - deleting, 208
- controlling
 - HP 9000 iLO iLO, 359
 - HP Integrity iLO, 359
- Copy Depot Software, 445
- copy file tool, 301
 - creating, 303
- copying
 - automatic event handling tasks, 509
 - reports, 481
 - tasks, 517
 - time filters, 286
- copyright, 32
- cp, 306
- CPU resource, 296, 300
- CPU thresholds, 292
- CPU utilization, 300
 - cluster monitor, 298
- Create or Modify Recovery Archive, 445
- Create or Modify Tape Recovery Archive, 445
- creating
 - authorizations, 132
 - automatic event handling task, 506, 508, 514, 538
 - automatic event handling tasks, 504, 509–510
 - cluster collections, 181
 - command line tool, 302
 - copy file tool, 303
 - CSR, 156
 - custom commands, 326–327
 - data collection task, 558
 - discovery hosts files, 91
 - discovery task, 76, 78
 - discovery templates, 86–87
 - event collection, 535, 537
 - event collections, 187
 - hosts files, 91–92
 - HP 9000 iLO user, 355
 - HP Integrity user, 355
 - replicate agent settings task, 376
 - reports, 478
 - rules, 106
 - server certificates, 150, 153
 - system collections, 181
 - task, 269, 273
 - time filters, 286
 - toolboxes, 128
 - users, 52, 117
 - Web launch tool, 333
 - X window tool, 305
- CSR (see Certificate Signing Request)
- custom command problems, 601
- custom commands, 288
 - creating, 327
 - deleting, 328
 - editing, 328–329
 - environment variables, 326
 - managing, 326, 328
 - naming conventions, 327, 329
 - removing, 326
 - running, 328
 - scheduling, 328
 - valid characters, 327, 329
 - web launch tool, 326
- custom tool
 - variables, 331
- customizing
 - cluster collections, 180–181
 - cluster table view, 215–216
 - cluster table view page, 220
 - event collections, 186
 - event table view, 223
 - event table view page, 227
 - system collections, 180–181
 - system status panel, 56
 - system table view, 192
 - system table view page, 207
 - Systems and Events panel, 175

D

- data collection, 36, 555
 - append new data set, 555
 - bi-weekly, 555
 - detailed analysis, 555
 - initial, 555
 - overwrite existing data set, 555
 - search criteria, 555
 - storage systems, 256
- data collection task
 - creating, 558
 - running, 558
 - scheduling, 555, 558
 - viewing results, 558
- data migration tool, 36
- database, 101, 601
 - adding systems, 91
 - administration, 220, 228
 - assigning events, 228
 - backing up SQL, 592
 - backup, 591
 - backup for HP-UX, 592
 - backup for Linux, 592
 - backup for Windows, 592
 - deleting clusters, 220
 - deleting events, 228
 - deleting system, 208
 - restoring, 591
 - systems, 727
 - views, 483
- default tasks
 - bi weekly data collection, 270
 - daily device identification, 270
 - hardware status polling for non servers, 270
 - hardware status polling for servers, 270
 - hardware status polling for systems no longer disabled, 270
 - initial data collection, 270
 - initial hardware status polling, 270
 - software version status polling, 270
 - software version status polling for systems no longer disabled, 270
- deleting
 - authorizations, 132, 138
 - automatic event handling tasks, 509
 - clusters, 215, 220
 - collections, 184
 - containers, 208
 - custom commands, 328
 - discovery task, 76, 80
 - discovery templates, 86, 88
 - disk thresholds, 337
 - event collections, 189
 - events, 228, 504, 522, 535, 537
 - hosts files, 91, 94
 - HP 9000 iLO user, 357
 - HP Integrity user, 357
 - management proxy host systems, 208
 - SSH keys, 588, 591
 - STM rule, 103, 110
 - systems, 192, 208
 - task, 269, 276, 280
 - task instance, 285
 - task results, 284
 - time filters, 286
 - toolboxes, 130
 - trusted certificates, 163, 166
 - user groups, 124
 - users, 124
 - WMI Mapper proxy, 208, 544, 546
- Deploy SSH Public Key, 445
- deploying
 - Deploying HP SIM on MSCS Clusters , 66
 - HP 9000 iLO SSH public key, 360
 - HP Integrity SSH public key, 360
 - license keys, 338, 342
 - VMM, 437
 - VMM Linux agent, 438
 - VMM Windows agent, 438
- desktop, 81
- df, 114
- DHCP server, 601
- disabling
 - automatic event handling tasks, 509, 519
 - discovery filters, 85
 - discovery task, 76, 80
- discovery, 50, 101, 568
 - automatic, 36, 52, 70, 76, 78–79, 84–86, 101, 210, 232, 260, 502, 547–548
 - automatic discovery, 100
 - Command View, 264
 - creating hosts files, 91
 - creating templates, 86
 - deleting hosts files, 91
 - editing hosts files, 91
 - event based auto-discovery, 70
 - first, 70
 - general settings, 84
 - IP ranges, 100
 - manual, 52, 70, 89, 502
 - storage solutions (SNMP), 264
 - storage systems, 256
 - templates, 70
- discovery command, 601
- discovery filters, 36, 84, 101
 - accessing, 85
 - disabling, 85

- editing, 85
 - discovery task
 - creating, 76, 78
 - deleting, 76, 80
 - disabling, 76, 80
 - editing, 76, 79
 - enabling, 76, 80
 - general settings, 76
 - running, 76, 81
 - scheduling, 78
 - stopping, 76, 81
 - discovery template
 - managing, 76
 - discovery templates, 70
 - creating, 86–87
 - deleting, 86, 88
 - editing, 86–87
 - Disk capacity, 300
 - Disk resource, 296, 300
 - disk thresholds, 292
 - example, 337
 - overview, 336
 - removing, 336
 - setting, 336–337
 - discovery
 - automatic discovery, 87
 - distributed task facility, 301, 306
 - DML, 84, 101, 383, 387, 543, 548, 555, 568, 70, 553
 - DML access
 - configuring, 288, 334
 - DML identification, 111
 - DML rule
 - adding, 111
 - deleting, 103
 - DML status polling, 541
 - document type definition
 - mxtool, 303, 305–306, 333
 - DTD (see document type definition)
 - DTF (see distributed task facility)
 - DTMF, 553
- E**
- e-mail
 - encoding, 510
 - html, 510
 - message format, 510
 - pager/SMS, 510
 - e-mail paging
 - examples, 528
 - e-mail settings, 50, 504, 506
 - automatic event handling tasks, 504
 - CMS, 520
 - configuring, 52, 520
 - SMTP host, 520
 - editing
 - authorizations, 132
 - automatic event handling tasks, 509
 - cluster collections, 183
 - custom commands, 328–329
 - discovery filters, 85
 - discovery task, 76, 79
 - discovery templates, 86–87
 - event collections, 188
 - hosts files, 91, 94
 - HP 9000 iLO user, 356
 - HP Integrity user, 356
 - MIB, 362
 - reports, 480
 - rules, 109
 - server certificates, 150, 152
 - system collections, 183
 - system properties, 36
 - task, 269, 276, 279
 - tasks, 517
 - time filters, 286
 - toolboxes, 129
 - user groups, 121
 - users, 121
 - WMI Mapper proxy, 544–545
 - enabling
 - automatic event handling tasks, 509, 519
 - discovery task, 76, 80
 - system monitoring, 36
 - enclosure, 81, 84, 101, 192, 204, 206, 223, 232
 - enclosure view, 204
 - English, 58
 - environment monitoring products, 446
 - environment variables
 - custom commands, 326, 331
 - environmental monitor, 81
 - event collection
 - creating, 535, 537
 - event collections
 - creating, 187
 - customizing, 186, 222
 - deleting, 189
 - editing, 188
 - HP Storage Essentials, 260
 - managing, 222
 - overview, 175
 - printing, 222, 230
 - report, 230
 - setting properties, 190
 - shared, 249
 - Event Monitoring Service, 446

- accessing, 454
 - overview, 454
 - event problems, 601
 - event search results
 - printing, 241
 - event status, 56
 - event table view
 - printing results, 223
 - event table view page, 175, 227–229, 232, 245, 382
 - adding columns, 227
 - customizing, 223, 227
 - deleting columns, 227
 - navigating, 223
 - overview, 222
 - printing, 230
 - sorting, 227
 - event tasks
 - examples, 533
 - event type, 232
 - event/SNMP trap, 601
 - events
 - adding comments, 222, 229
 - administering, 504, 506, 508
 - assignee, 232
 - assigning, 222, 228
 - associated system, 232
 - change details, 232
 - cleared status, 232
 - clearing, 222, 227, 504, 522, 535
 - comments, 232
 - configuring, 148, 526
 - configuring filters, 523
 - creating tasks, 510
 - deleting, 222, 228, 241, 504, 506, 522, 535, 537
 - description, 232
 - details, 223, 232
 - filter settings, 504
 - filtering settings, 506
 - filters, 523
 - HP Storage Essentials, 260
 - managing tasks, 509
 - modem settings, 521
 - monitoring, 174
 - print details, 232
 - rules, 506
 - searching, 234, 239
 - server, clearing, 535
 - service, 249
 - service notifications, 530
 - severity, 223, 231–232
 - SNMP trap settings, 504
 - SNMP traps, 524
 - source, 232
 - status, 223, 526
 - status change, 526
 - storage (SNMP), 261
 - storage solutions (SNMP), 265
 - time, 223, 232
 - type, 223
 - uncleared status, 178
 - view details, 232
 - events collections
 - printing, 222
 - events task
 - running, 535
 - scheduling, 535
 - examples, 160, 568
 - clearing server events, 535
 - command line tool parameters, 325
 - delete cleared events, 533
 - delete informational events, 533
 - deleting disk thresholds, 337
 - e-mail paging, 528
 - send e-mail, 533
 - web launch tool parameters, 325
 - execute-as user, 568, 601
 - exporting
 - server certificates, 151
 - SSH keys, 588, 590
 - trusted certificates, 163, 165
- ## F
- fault management, 36
 - filter settings
 - events, 504
 - filtering
 - event settings, 506
 - filters
 - configuring, 523
 - firmware upgrade, 601
 - firmware upgrade problems, 601
 - first time wizard, 36, 46, 50
- ## G
- generic, 601
 - generic problems, 601
 - Get Patch Catalog, 446
 - getting started, 46
 - GlancePlus Pak
 - overview, 455
 - global protocol settings, 76, 547–548
 - setting, 84, 555
 - storage systems, 256
 - globalsettings.props, 58, 149, 526, 596
 - graphical user interface, 36

- banner, 53
 - customize Home page, 55
 - customizing system status panel, 56
 - Home page, 53
 - overview, 53
 - groups, 132
 - GUI (see graphical user interface)
- ## H
- handheld, 81
 - hardware status, 192
 - hardware status polling, 543, 548
 - running, 543
 - scheduling, 543
 - hardware status polling for non-servers, 541
 - hardware status polling for servers, 541
 - health status, 56, 178, 383, 387
 - types, 210
 - health status section, 53
 - help, 44
 - Home page, 53
 - customize, 55
 - overview, 53
 - hosts file
 - creating, 92
 - hosts files
 - , 70
 - add system, 70
 - adding systems, 91
 - adding to database, 95
 - creating, 91
 - deleting, 91, 94
 - editing, 91, 94
 - extensions, 97
 - importing, 95
 - HP 9000 iLO, 353, 446
 - controlling iLO, 359
 - creating user, 355
 - deleting user, 357
 - deploying SSH public key, 360
 - editing user, 356
 - LAN access, 358
 - LDAP settings, 358
 - system locator, 355
 - system power, 354
 - upgrading firmware, 360
 - HP Array Configuration Utility
 - accessing, 466
 - overview, 466
 - HP BladeSystem Integrated Manager
 - overview, 468
 - HP BladeSystem Integrated Manager in HP Systems Insight Manager, 36
 - accessing, 468
 - HP business desktops, 446
 - HP Client Manager, 446
 - accessing, 468
 - overview, 468
 - HP Configure or Repair Agents, 36
 - HP Insight Management Agent, 601
 - HP Instant Tootools, 192
 - HP Integrity, 353, 446
 - controlling iLO, 359
 - creating user, 355
 - deleting user, 357
 - deploying SSH public key, 360
 - editing user, 356
 - LAN access, 358
 - LDAP settings, 358
 - system locator, 355
 - system power, 354
 - upgrading firmware, 360
 - HP Integrity Essentials Capacity Advisor, 469
 - HP Integrity Essentials Virtualization Manager, 469
 - HP Integrity Global Workload Manager, 469
 - HP Integrity Integrated Lights Out, 353
 - HP Integrity servers
 - Integrated Lights-Out, 456
 - HP Integrity Superdome, 81
 - HP notebooks, 446
 - HP OpenView Network Node Manager , 36
 - HP OpenView Operations, 36
 - HP OpenView Performance Agent
 - overview, 461
 - HP OpenView Storage Area Manager
 - overview, 461
 - HP OpenView Storage Data Protector, 446
 - accessing, 460
 - overview, 460
 - HP OpenView Storage Management Appliance
 - accessing, 462
 - overview, 462
 - HP OpenView Storage Operations Manager
 - accessing, 463
 - overview, 463
 - HP Performance Management Pack, 36, 288, 567
 - accessing, 567
 - configuring, 567
 - licensing, 567
 - manual log purge, 567
 - HP ProLiant Essentials, 464
 - HP ProLiant Essentials Automation Manager
 - overview, 467
 - HP ProLiant Essentials Performance Management Pack, 192, 338, 342
 - accessing, 373

- HP ProLiant Essentials Rapid Deployment Pack - Windows Edition, 36
 - HP ProLiant Essentials Server Migration Pack, 36, 288, 380–381
 - HP ProLiant Essentials Virtual Machine Management Pack, 36, 192, 288, 380, 437–438, 441
 - accessing, 437
 - deploying, 437
 - HP ProLiant Essentials Vulnerability and Patch Management Pack, 36, 192
 - accessing, 469
 - HP Serviceguard Cluster, 288
 - HP Serviceguard cluster, 216, 458
 - HP Serviceguard Manager, 36, 458
 - HP SIM, 601
 - commands, 62
 - public key, 368
 - setting up, 52
 - HP SIM commands, 62
 - HP SIM Overview, 36
 - HP SIM problems, 601
 - HP Storage Essentials, 36, 446
 - accessing, 470
 - affect on reports, 258
 - collections, 249
 - data collection report, 417
 - discovery, 76
 - events, 229, 522
 - overview, 470
 - storage array Identity tab, 409
 - storage host Identity tab, 404
 - storage switch Identity tab, 407
 - Suspend/Resume Monitoring, 564
 - system properties, 559, 562
 - tape library Identity tab, 413
 - toolboxes, 127
 - using with HP Systems Insight Manager, 260
 - HP StorageWorks Command View EVA, 446
 - accessing, 472
 - overview, 472
 - HP StorageWorks Command View SDM, 446
 - accessing, 471
 - overview, 471
 - HP StorageWorks Command View TL, 446
 - accessing, 472
 - overview, 472
 - HP StorageWorks Command View XP, 446
 - accessing, 471
 - overview, 471
 - HP StorageWorks Command View XP Advanced Edition, 446
 - accessing, 471
 - overview, 471
 - HP StorageWorks EVA, 446
 - HP StorageWorks MA/EMA, 446
 - HP StorageWorks Modular Smart Array 1000
 - accessing, 473
 - overview, 473
 - HP StorageWorks Modular Storage Array 1000, 446
 - HP StorageWorks XP, 446
 - HP StorageWorksVA, 446
 - HP System Management Homepage, 36
 - HP tablet PCs, 446
 - HP Virtual Server Environment
 - accessing, 469
 - overview, 469
 - HP Web Jetadmin
 - accessing, 470
 - overview, 470
 - HP workstations, 446
 - HP-UIX, 599
 - HP-UX, 159, 301, 306, 543, 555, 601
 - commands, 114
 - configuring language, 58
 - configuring PAM, 143
 - restoring database, 592
 - use authorization, 143
 - viewing MIB list, 361
 - HP-UX Bastille
 - overview, 455
 - HP-UX commands, 300
 - HP-UX Configuration, 446
 - HP-UX SAM, 446
 - HP-UX systems
 - WBEM indications, 36
 - HTTP, 84, 101, 205, 232, 543
 - HTTP event problems, 601
 - HTTP events, 601
 - HTTPS, 84
 - hub, 81
- I**
- ICMP, 548
 - ICMP Settings, 550–551
 - icon view, 202
 - identification, 36, 205, 601
 - cluster, 541
 - DMI, 111
 - initial, 101
 - management processor, 541
 - SNMP, 111
 - storage solutions (SNMP), 264
 - system, 101, 502
 - identification problems, 601
 - identity tab
 - cluster, 399
 - complex, 400

- management processor, 387
 - partition, 402
 - server, 383
 - storage array, 409
 - storage host, 404
 - storage switch, 407
 - tape library, 413
 - virtual machine host, 388
 - VM guest, 390
 - Ignite-UX, 306, 446
 - accessing, 456
 - overview, 456
 - Ignite-UX Console, 445
 - Ignite-UX Restricted Console, 445
 - iLO, 81, 84, 101, 192, 210, 456 (see Integrated Lights-Out)
 - associating with a server, 601
 - configuring, 350
 - importing
 - CSR, 158
 - hosts file, 95
 - server certificates, 150, 155
 - SSH keys, 588, 590
 - submitting CSR, 157
 - trusted certificates, 163–164
 - initial data collection, 555
 - initial ProLiant Pack install, 36
 - Initial ProLiant Support Pack Install, 445
 - initial setup, 52
 - initial status polling, 101
 - Insight Manager 7, 555
 - Install OpenSSH, 445
 - Install or Recover System, 445
 - Install Software, 445
 - Install WLM Configuration, 445
 - installation, 36, 601
 - installation problems, 601
 - installing
 - Installing and using the HP ProLiant Essentials Performance Management Pack Data Migration Tool, 66
 - Installing HP SIM, 66
 - Installing the System Management Homepage individually, 66
 - Installing version control individually , 66
 - OpenSSH, 366, 368
 - OpenSSH tool, 36
 - ProLiant Support Pack, 430
 - RPM Package Manager, 378
 - Instant Support Enterprise Edition, 446, 530
 - Integrated Lights-Out, 210
 - accessing, 456
 - HP Integrity servers, 456
 - overview, 456
 - integrated Lights-Out Advanced, 446
 - integrated Lights-Out Standard, 446
 - integration, 421
 - Integrity Essentials, 450
 - Internet Explorer, 601
 - language, 58
 - Internet Explorer problems, 601
 - IP, 84, 383
 - IP address, 335, 601
 - IP address problems, 601
 - IP ranges
 - reference, 100
 - specifying, 84
 - IPX, 383
 - IPX address, 335
 - IPX SAP, 84
 - ISEE (see Instant Support Enterprise Edition)
- ## J
- Japanese, 58
 - java, 601
- ## K
- kernel configuration, 446
 - kernel parameters, 601
 - keys, 338
 - keystore, 159
 - known_hosts file, 588
 - KVM switch, 81
- ## L
- LAN access
 - HP 9000 iLO, 358
 - HP Integrity, 358
 - language
 - English, 58
 - Internet Explorer, 58
 - Japanese, 58
 - Mozilla, 58
 - setting, 58
 - launching
 - application, 326
 - custom commands, 326
 - VM remote console, 391
 - LDAP settings
 - HP 9000 iLO, 358
 - HP Integrity, 358
 - learning
 - Learning more about the ProLiant or Integrity Support Packs., 66
 - Learning more about the ProLiant Remote Deployment Utility, 66
 - legal notices, 32

- legend, 53
 - licene keys
 - managing, 345
 - license database
 - viewing contents, 346
 - license keys, 341, 344
 - activation key agreement, 339
 - adding from file, 347
 - adding individually, 348
 - demo, 339
 - demo (seats and time), 339
 - deploying, 342
 - evaluation, 339
 - flexible quantity, 339
 - iLO, 345
 - individual, 339
 - intrinsic, 339
 - managing, 352
 - selecting, 343
 - subscription, 339
 - viewing details, 349
 - license management, 338, 352
 - license manager, 288, 341
 - licenses
 - reporting, 350
 - licensing
 - about keys, 339
 - adding keys from file, 347
 - adding keys individually, 348
 - collecting keys, 338, 341
 - collection results, 341
 - deploying keys, 338, 342
 - deployment results, 344
 - iLO, 338
 - managing keys, 338, 345
 - PMP, 567
 - ProLiant Essentials, 338
 - selecting keys, 343
 - SMP, 380
 - view details, 349
 - viewing database contents, 346
 - Linux, 159, 301, 438, 543, 555, 599, 601
 - commands, 114
 - configuring language, 58
 - restoring database, 592
 - use authorization, 143
 - VCA, 419
 - viewing MIB list, 361
 - Linux commands, 300
 - Linux systems
 - WBEM indications, 36
 - lists
 - task results, 284
 - locale
 - English, 58
 - Japanese, 58
 - log.properties, 597, 599
 - logging in
 - CLI, 46
 - login, 142, 601
 - configuring events, 148
 - failure, 143
 - single, 143
 - login events
 - settings, 148
 - login problems, 601
 - logs
 - all scheduled tasks, 280
 - ls, 114, 306
- ## M
- Manage SSH Keys, 588
 - manage system types page
 - navigating, 103
 - managed system, 43
 - overview, 43
 - managed systems, 160, 430
 - Automating Software Maintenance in an HP Environment, 66
 - overview, 568
 - setting up, 568
 - management, 423
 - management agents, 192, 568
 - management domain
 - overview, 43
 - Management HTTP Server
 - trust relationships, 168
 - management processor, 81, 101, 192, 205, 288, 383, 387
 - identification, 541
 - identity tab, 387
 - management processors
 - creating user, 353
 - deleting user, 353
 - deploying SSH public key, 353
 - editing user, 353
 - iLO control, 353
 - LAN access, 353
 - LDAP settings, 353
 - system locator, 353
 - system power, 353
 - upgrading firmware, 353
 - management protocols, 568, 553
 - management proxies
 - deleting host systems, 208
 - managing

- automatic event handling task, 506
 - automatic event handling tasks, 504, 509
 - cluster collections, 215
 - custom commands, 326, 328
 - discovery task, 76
 - events, 504
 - license keys, 338, 345, 352
 - Managing HP servers through firewalls with HP SIM, 66
 - Managing WBEM Event Subscriptions for HP-UX Systems with HP SIM, 66
 - reports, 481
 - SSH keys, 36, 589
 - system groups from CLI, 140
 - system groups from GUI, 140
 - system types, 102
 - time filters, 286
 - manual discovery, 52
 - adding system, 89
 - hosts files, 70
 - mcompile, 62, 362
 - MIB, 111, 288, 530
 - compiling, 364
 - editing, 362
 - internet management, 553
 - preloaded, 365
 - registering, 361, 365
 - rules, 111
 - unregistering, 366
 - vendor, 553
 - viewing list, 361, 365
 - MIF
 - example, 111
 - migrating
 - Manually Migrating to HP SIM, 66
 - Moving HP SIM to a new system, 66
 - modem settings, 504, 506
 - automatic event handling tasks, 504
 - configuring, 521
 - monitoring (see enabling) (see suspending)
 - clusters, 174
 - events, 174
 - MSCS status, 296
 - systems, 174
 - Mozilla, 601
 - language, 58
 - MSA (see multiple-system aware) (see multiple-system aware tools)
 - MSA tools, 288, 445
 - MSCS
 - clusters, 291
 - MSCS polling rate, 292
 - MSCS resource, 296
 - MSCS status
 - monitoring, 296
 - multiple-system aware tools, 58, 306
 - multiple-system aware, 281, 284
 - mx.log, 599
 - mxagentconfig, 36, 62, 302–303, 305, 357, 366
 - mxauth, 62, 133, 138–139
 - mxcert, 62
 - mxcollection, 62, 181, 183–189
 - mxdomainmgr, 62
 - mxdtf, 62, 596
 - mxexec, 58, 62, 117, 119, 121, 124–125, 128–131, 133, 138–139, 273, 279, 300, 526
 - mxgethostname, 62
 - mxglobalprotocolsettings, 62
 - mxglobalsettings, 62
 - mxinitconfig, 62
 - mxmib, 62, 361, 366
 - mxngroup, 62, 133, 136, 139–140
 - mxnode, 62, 89, 138
 - mxnodesecurity, 62
 - mxpassword, 62
 - mxquery, 62
 - mxreport, 62, 475, 478, 480–481
 - mxstart, 62
 - mxstm, 62, 104, 106, 109–111
 - mxstop, 62, 599
 - mxtart, 599
 - mxtask, 58, 62, 279, 285, 526, 558
 - mxtool, 62, 302–303, 305, 333, 357
 - document type definition, 303
 - document type definition, 305–306, 333
 - other requirements, 303, 305–306, 333
 - parameterized strings, 303, 305–306, 333
 - strings substitution table, 303, 305–306, 333
 - tool filtering, 303, 305–306, 333
 - tool types, 303, 305–306, 333
 - version numbers, 303, 305–306, 333
 - mxtoolbox, 62, 128–131
 - mxuser, 62, 117, 119, 121, 124–125
 - mxwbemsub, 62, 526
- ## N
- naming conventions
 - custom commands, 327, 329
 - navigating
 - All Scheduled Tasks page, 276
 - cluster table view page, 216
 - event table view page, 223
 - Home page, 53
 - manage system types page, 103
 - picture view page, 204
 - system table view page, 192
 - Systems and Events panel, 175

network client
 overview, 43
 network clients, 43
 node status, 294
 nodes
 status, 294
 notebook, 81

O

Open Service Event Manager, 446, 530
 OpenSSH, 288, 368, 370, 430, 438, 526, 601
 command line, 370
 install, 36
 installing, 366, 368
 OpenSSH problems, 601
 OpenSSH tool
 installing, 36
 OpenSSL, 159, 601
 operating system, 192, 601
 name, 101, 192
 type, 101
 version, 101
 operator-template, 126
 OS name, 192
 OSEM (see Open Service Event Manager)
 other requirements
 mxtool, 303, 305–306, 333
 overview, 163, 338
 authorizations, 114
 backup, 591
 Event Monitoring Service, 454
 GlancePlus Pak, 455
 HP Array Configuration Utility, 466
 HP BladeSystem Integrated Manager in HP Systems
 Insight Manager, 468
 HP Client Manager, 468
 HP OpenView Performance Agent, 461
 HP OpenView Storage Area Manager, 461
 HP OpenView Storage Data Protector, 460
 HP OpenView Storage Management Appliance,
 462
 HP OpenView Storage Operations Manager, 463
 HP ProLiant Essentials Automation Manager, 467
 HP Storage Essentials, 470
 HP StorageWorks Command View EVA, 472
 HP StorageWorks Command View SDM, 471
 HP StorageWorks Command View TL, 472
 HP StorageWorks Command View XP, 471
 HP StorageWorks Command View XP Advanced
 Edition, 471
 HP StorageWorks Modular Smart Array 1000, 473
 HP Web Jetadmin, 470
 HP-UX Bastille, 455

Ignite-UX, 456
 Integrated Lights-Out, 456
 managed systems, 568
 Partition Manager, 457
 reporting, 474
 security, 142
 Security Patch Check, 457
 service notifications, 530
 Software Distributor, 459
 storage solutions (SNMP), 261
 storage systems, 255
 System Fault Management, 443
 version control, 418
 VPM, 469
 VSE, 469
 WBEM Providers for Linux, 444
 WMI Mapper proxy, 544
 Workload Manager, 460
 overwrite existing data set
 append new data set, 558

P

pager settings
 configuring, 52
 pager support, 36
 paging notification, 601
 paging notification problems, 601
 PAM (see Pluggable Authentication Modules)
 parameterized strings
 mxtool, 303, 305–306, 333
 strings substitution table, 303, 305–306, 333
 parameters
 examples, 325
 partition, 81
 identity tab, 402
 partition management, 446
 Partition Manager, 446
 accessing, 457
 overview, 457
 path.properties, 599
 pausing
 VM guest, 394
 Performance Management Pack, 446
 permissions, 133
 Personal Digital Assistant, 81
 picture view page, 206
 navigating, 204
 ping, 335
 alternate, 36
 settings, 548
 ping problems, 601
 plug-in tools, 378, 446, 456
 Event Monitoring Service, 454

- HP Array Configuration Utility, 466
- HP BladeSystem Integrated Manager in HP Systems Insight Manager, 468
- HP Integrity Integrated Lights Out, 353
- HP OpenView Performance Agent, 461
- HP OpenView Storage Area Manager, 461
- HP OpenView Storage Data Protector, 460
- HP OpenView Storage Management Appliance, 462
- HP OpenView Storage Operations Manager, 463
- HP ProLiant Essentials Automation Manager, 467
- HP Storage Essentials, 260, 470
- HP StorageWorks Command View EVA, 472
- HP StorageWorks Command View SDM, 471
- HP StorageWorks Command View TL, 472
- HP StorageWorks Command View XP Advanced Edition, 471
- HP StorageWorks Modular Smart Array 1000, 473
- HP Web Jetadmin, 470
- HP-UX Bastille, 455
- JHP StorageWorks Command View XP, 471
- Partition Manager, 457
- Software Distributor, 459
- System Fault Management, 443
- VPM, 469
- VSE, 469
- WBEM Providers for Linux, 444
- Pluggable Authentication Modules, 143
 - configuring, 143
- PMP, 36, 192, 288, 342, 502, 567 (see HP ProLiant Essentials Performance Management Pack) (see Performance Management Pack)
 - CSV file generator, 500
 - offline analysis, 373
 - online analysis, 373
- polling rate
 - cluster resource, 292
- polling tasks
 - customizing, 541
 - default, 270
- port 25, 601
- PostgreSQL DB Backup, 445
- power distribution unit, 81
- power management software, 446
- power supply, 81
- printer, 81
- printer management software, 446
- printing, 601
 - cluster collections, 215
 - cluster table view, 216
 - event table view, 223
 - reports, 475, 478, 480
 - system table view, 192
 - task results, 283
 - printing problems, 601
 - printing results
 - canceling, 209, 221, 230
 - cluster search, 244
 - cluster table view page, 221
 - event search, 241
 - event table view page, 230
 - system search, 239
 - system table view page, 209
 - printing search results
 - canceling, 239, 241, 244
 - private collections, 175
 - Process Resource Manager, 288, 463
 - accessing, 463
 - product architecture, 43
 - product name, 101, 192
 - program
 - launching, 326
 - program launch tool, 288
 - program launch tools, 306
 - ProLiant Essentials Vulnerability and Patch Management Pack, 446
 - overview, 469
 - ProLiant Support Pack, 568
 - installing, 430
 - property pages, 36
 - accessing, 442
 - WBEM, 36, 442
 - protocol problems, 601
 - protocol settings
 - configuring, 52
 - protocols, 568
 - configuring, 550–551
 - DMI, 70, 101, 543, 548, 553, 555
 - global, 547
 - group, 550
 - HTTP, 101, 205, 232, 543, 553
 - ICMP, 548
 - IP, 70
 - IPX, 70
 - setting, 547
 - setting global, 84, 256, 548
 - single system, 547, 550–551
 - SNMP, 70, 101, 205, 232, 541, 543, 548, 553, 555
 - SSH, 101
 - TCP, 548
 - WBEM, 70, 101, 548, 553, 555
 - WMI Mapper proxy, 544–546
 - public key, 588
 - security level, 588

Q

querying
 RPM Package Manager, 378–379

R

R_ArrayControllers, 483
 R_Batteries, 483
 R_CellularSysParComplex, 483
 R_CellularSysParIOChassis, 483
 R_CellularSysPartition, 483
 R_CPU, 483
 R_deviceLicenseInfo, 483
 R_DIMMSlots, 483
 R_HPUXFileSystem, 483
 R_HPUXKernelParam, 483
 R_HPUXLogicalVolume, 483
 R_HPUXNetworkDetails, 483
 R_HPUXPhysicalVolume, 483
 R_HPUXSoftwareBundle, 483
 R_HPUXSoftwareProduct, 483
 R_HPUXVolumeGroup, 483
 R_InstalledBoards, 483
 R_Inventory, 483
 R_lockdownStatus, 483
 R_LogicalDisks, 483
 R_NetworkInterface, 483
 R_OperatingSystem, 483
 R_PhysicalDisks, 483
 R_PowerSupply, 483
 R_Process, 483
 R_Racks, 483
 R_Software, 483
 R_StorageDeviceCapacity, 483
 R_StorageDeviceControllers, 483
 R_StorageDeviceInventory, 483
 R_StorageHostBusAdapters, 483
 R_StorageLogicalUnits, 483
 R_StoragePorts, 483
 R_UnixIODevices, 483
 R_UnixIPRoute, 483
 R_UnixLogicalMemory, 483
 R_UnixOSDetails, 483
 rack, 81, 84, 204, 206, 223, 232
 Rack and Power Manager, 446
 rack view, 204
 Rapid Deployment Pack, 368, 446
 RDP, 36
 receiving
 Receiving alerts, 66
 reference
 commands, 62
 registering
 MIB, 361, 365
 VM host, 440
 release history, 32
 remote access device, 81
 Remote Insight Board EISA, 205
 Remote Insight Board PCI, 205
 Remote Insight Lights-Out Edition, 446
 Remote Insight Lights-Out Edition (RILOE), 205
 Remove Depot Software, 445
 Remove Software, 445
 remove tool, 301
 running, 374
 removing
 custom commands, 326
 disk thresholds, 336
 Replicate Agent Settings, 160, 288
 replicate agent settings
 accessing, 375
 creating task, 376
 events, 377
 trust relationship, 375, 377
 Replicate Agent Settings problems, 601
 replicating, 160, 376
 reporting, 499–500, 601, 644
 creating a report, 478
 editing a report, 480
 license, 350
 license information, 350
 overview, 474
 running reports, 475
 SQL queries, 482
 storage array capacity, 259
 storage systems, 258
 views, 350, 474, 482–483
 reporting problems, 601
 reports, 36, 474, 500
 authorizations, 139
 copying, 481
 creating, 478
 editing, 480
 license information, 350
 managing, 481
 printing, 475, 478, 480
 running, 475
 showing SQL, 482
 snapshot comparison, 36
 sort order, 475, 478, 480
 storage systems, 258
 toolbox, 131
 user, 125
 user groups, 125
 views, 483
 with HP Storage Essentials installed, 258
 resetting
 VM guest, 393

- resource library, 66
 - Changing the HP SIM system name, 66
 - HP StorageWorks Management Software, 66
 - Using OpenView, 66
 - Using the HP ProLiant Essentials Server Migration Pack, 66
 - resources
 - assistance, 44
 - cluster monitor, 296, 300
 - thresholds, 300
 - response, 601
 - response problems, 601
 - restoring
 - database, 591
 - Retrieve WLM Configuration, 445
 - rights, 114
 - router, 81, 101
 - RPM (see RPM Package Manager)
 - RPM Package Manager, 378, 446
 - accessing, 378
 - installing, 378
 - querying, 378–379
 - uninstalling, 378–379
 - verifying, 378, 380
 - rules
 - creating, 106
 - DML, 111
 - editing, 109
 - SNMP, 111
 - STM, 111
 - running
 - clear events task, 522
 - custom commands, 328
 - data collection task, 558
 - discovery task, 76, 81
 - events task, 535
 - remove tool, 374
 - reports, 475
 - task, 276, 279
- S**
- SAM, 446
 - saving
 - collection, 179
 - collections, 535
 - system collection, 192
 - scheduling
 - clear events task, 522, 535
 - custom commands, 328
 - data collection task, 558
 - discovery task, 78
 - event tasks, 535, 537
 - task, 269, 277
 - script launch tool, 288
 - script launch tools, 306
 - SD Job Browser, 445
 - search, 53
 - saving, 179
 - system, 179
 - search criteria, 206, 223, 245, 543, 555
 - cluster, 245
 - event, 245
 - system, 245
 - search problems, 601
 - searching, 601
 - advanced, 234–235, 237, 239, 242
 - basic, 234–236
 - clusters, 242
 - criteria, 245
 - deleting clusters, 243
 - deleting events, 241
 - deleting systems, 238
 - event, 234
 - events, 239
 - hierarchical displays, 235
 - system, 234
 - systems, 237
 - secure shell, 36, 588
 - install, 36
 - Secure Sockets Layer, 142
 - secure sockets layer, 36
 - Secure Task Execution, 147
 - secure task execution, 168
 - security, 159, 601
 - about trust relationships, 168
 - login, 143
 - login event settings, 148
 - options, 142
 - overview, 142
 - role-based, 36
 - secure task execution, 147
 - System Link Configuration, 148
 - timeout, 149
 - security alert, 601
 - security level
 - SSH keys, 589
 - security management, 446
 - Security Patch Check, 446
 - overview, 457
 - security problems, 601
 - selecting
 - license keys, 343
 - server, 81
 - identity tab, 383
 - server blade, 383
 - server certificate, 160
 - Server Certificate page, 150

- server certificates, 150, 156–159
 - creating, 150, 153
 - editing, 150, 152
 - exporting, 151
 - importing, 150, 155
 - synchronizing, 159
- server monitoring, 446
- service and support, 728
- service events (see service notifications)
- service notifications
 - configuring, 530
 - details, 530
 - overview, 530
- Serviceguard Manager, 192, 446, 601
- Serviceguard Manager problems, 601
- setting
 - disk thresholds, 336
 - global protocols, 84
 - language, 58
 - locale, 58
 - ping, 548
 - trust relationships, 168
- setting properties
 - cluster collections, 185
 - event collections, 190
 - system collections, 185
- setting up
 - HP SIM, 52
 - managed systems, 568
- settings
 - disk thresholds, 337
 - login event, 148
- setup
 - initial, 52
- severity
 - event, 231
- shared collections, 175, 249
- signing in
 - GUI, 46
 - remotely, 46
 - using SSL, 46
- signing out
 - CLI, 50
 - GUI, 50
- single login, 143, 168
- single system protocol settings, 547
 - setting, 555
- single-system aware tools, 58, 281, 306
- Smart Array controllers, 446
- SMI CIMOM, 548
- SMI-S providers
 - storage systems, 256
- SMI-S systems
 - WBEM indications, 36
- SMP (see HP ProLiant Essentials Server Migration Pack)
 - accessing, 381
 - adding license, 380
 - licensing, 380
- SMTP settings, 520
- snapshot comparison, 36, 499
- snapshot comparisons, 558
- SNMP, 50, 84, 101, 205, 232, 383, 387, 458, 541, 543, 548, 555, 568, 588–591
 - rules, 104
 - trap, 232, 504, 506
- SNMP access
 - configuring, 288, 335
- SNMP agent, 601
- SNMP agent problems, 601
- SNMP rule
 - adding, 111
 - deleting, 103
- SNMP Settings, 550–551
- SNMP status polling, 205
- SNMP trap, 223, 541
- SNMP trap problems, 601
- SNMP trap settings
 - events, 504
- SNMP traps, 506, 530
 - configuring, 524
 - fields, 524
- SOAP, 306
- Socks, 601
- software
 - administering, 502
 - status, 214
- Software Distributor, 36, 446
 - accessing, 459
 - overview, 459
 - VMM, 459
- Software Distributor Job Browser, 445
- software status, 192, 383, 601
- software status polling, 542
- software status problems, 601
- specifying
 - ip ranges, 84
- SQL
 - backing up database, 592
- SQL queries, 482
- SSA (see single-system aware tools)
- SSH, 36, 58, 101, 568, 588, 590 (see secure shell)
 - public key, 302–303, 305
 - Using SSH, 66
- SSH bypass properties
 - configuring, 596
- SSH Keys
 - deleting, 591
- SSH keys, 588

- deleting, 588
- exporting, 588, 590
- importing, 588, 590
- managing, 36, 589
- security level, 588
- SSH security level, 589
- SSH Settings, 550–551
- SSL (see Secure Sockets Layer) (see secure sockets layer)
- start using, 46
- starting
 - VM guest, 392
- status
 - event, 56
 - health, 178
 - node, 294
 - software, 214
 - system, 210
 - uncleared event, 178
 - WBEM status, 212
- status polling
 - hardware, 548
 - hardware status polling, 541
 - initial, 101
 - SNMP, 205
 - software status polling, 541
- STE (see Secure Task Execution)
- STM (see system type manager)
- STM rule
 - adding, 103
 - deleting, 103
- STM rule reference, 111
- stopping
 - discovery task, 76, 81
 - task, 269, 284–285
 - VM guest, 395
- storage array
 - identity tab, 409
- storage device, 81
- storage host
 - identity tab, 404
- storage integration
 - overview, 255
- storage solutions (SNMP)
 - about, 261
 - configuring event collection, 265
 - discovery, 264
 - overview, 255, 261, 265
 - searching for, 265
- storage switch
 - identity tab, 407
- storage system problems, 601
- storage systems (SMI-S)
 - discovery, 256
 - overview, 255
 - SMI-S providers, 256
 - storage systems, 258
 - viewing, 257
 - viewing array capacity, 259
 - WBEM event indications, 256
 - with HP Storage Essentials, 260
- submitting
 - CSR, 157
- Subscribe to WBEM Events, 445
- subscribing
 - WBEM events, 504, 527
 - WBEM indication events, 256
 - WBEM indications, 526
- Superdome, 36
- support, 44
- suspending
 - system monitoring, 36
- switch, 81, 101, 192, 601
- switch problems, 601
- synchronizing
 - server certificates, 159
- Syntax Check Configuration, 445
- Syntax Check on the Systems Insight Manager Server Configuration, 445
- system, 601
 - categories, 178
 - identification, 502
 - port types, 416
 - search, 179
 - searching, 234
 - status, 210
 - WBEM status, 212
- system address, 192
- System and Events panel
 - navigating, 175
- system collections
 - creating, 181
 - customizing, 180–181, 191
 - deleting, 184
 - editing, 183
 - managing, 191
 - overview, 175
 - printing, 191, 209
 - report, 209
 - setting properties, 185
 - shared, 249
- System Fault Management, 446
 - accessing, 443
 - overview, 443
- system groups
 - managing, 140
- system key, 53
- system locator

- HP 9000 iLO, 355
 - HP Integrity, 355
 - System Management Homepage, 381
 - accessing, 382
 - trust relationships, 168
 - system monitoring
 - resume, 36, 559
 - resume multiple systems, 565
 - resume single system, 564
 - suspend, 36, 559
 - suspend multiple systems, 565
 - suspend single system, 564
 - when HP Storage Essentials is installed, 260
 - system name, 192, 223
 - system overview, 174
 - System Overview page
 - viewing, 178
 - system page, 204–205, 223, 265, 383, 387–388, 390–397, 399–400, 402, 404, 407, 409, 413, 442, 547, 555, 601
 - event, 382
 - identity, 382
 - links, 382, 417
 - system power
 - HP 9000 iLO, 354
 - HP Integrity, 354
 - system problems, 601
 - system properties
 - edit, 36
 - edit for single system, 560
 - editing, 36
 - set for multiple systems, 562
 - when HP Storage Essentials is installed, 260
 - system resource, 296
 - system search results
 - printing, 239
 - system status, 175
 - system status panel, 53
 - customizing, 56
 - system subtypes, 404, 407, 409, 413
 - when HP Storage Essentials is installed, 260
 - system table view
 - printing results, 192
 - system table view page, 84, 95, 175, 204–206, 208, 216, 235, 265, 335, 382, 446, 458, 555, 601
 - adding columns, 207
 - customizing, 192, 207
 - deleting columns, 207
 - deleting systems, 192
 - navigating, 192
 - overview, 191
 - printing, 209
 - saving collection, 192
 - sorting, 207
 - system type, 84, 192
 - System Type Manager, 81
 - system type manager, 104, 102
 - creating new rule, 106
 - deleting rule, 110
 - DML rules, 111
 - editing SNMP rule, 109
 - SNMP rules, 111
 - system types, 81
 - systems, 341, 345
 - configuring links, 148
 - deleting, 191, 208, 238
 - identification, 101
 - monitoring, 174
 - searching, 237
 - Systems and Events panel
 - tree controls, 175
- ## T
- tape library
 - identity tab, 413
 - target system
 - task schedule, 273
 - task instance, 269
 - deleting, 285
 - viewing, 281
 - task problems, 601
 - task results
 - automatic event handling tasks, 509
 - deleting, 284
 - printing, 283
 - viewing, 276–277, 281, 284, 522, 535, 537
 - task results list, 284
 - task instance, 284
 - tasks, 36, 273, 601
 - copying, 517
 - creating, 269, 273
 - data collection, 555
 - default, 270
 - deleting, 269, 276, 280
 - details, 232
 - editing, 269, 276, 279, 517
 - instance, 269
 - paging, 533
 - polling, 270
 - replicate agent settings, 376
 - running, 276, 279
 - scheduling, 269, 277
 - status, 287
 - stopping, 269, 284–285
 - time filtering, 286

- track status, 269
 - user privileges, 269, 276
 - viewing, 281
 - viewing configuration, 518
 - viewing results, 519
 - TCP, 548
 - TDEF (see tool definition files)
 - template
 - users, 126
 - thin client, 81
 - thresholds
 - cluster monitor, 300
 - time filters, 286
 - applying, 277, 286, 510, 514, 533, 538
 - copying, 286
 - creating, 286
 - deleting, 286
 - editing, 286
 - managing, 286
 - timeout
 - configuring options, 149
 - setting, 543
 - tool definition files, 36, 597
 - tool filtering
 - mxtool, 303, 305–306, 333
 - tool problems, 601
 - tool types
 - mxtool, 303, 305–306, 333
 - toolbox
 - report, 131
 - toolboxes, 114, 128, 132
 - create, 127
 - creating, 128
 - delete, 127
 - deleting, 130
 - edit, 127
 - editing, 129
 - HP Storage Essentials, 127, 260
 - reports, 127
 - tools, 36, 424–425, 601
 - assistance, 446
 - cluster monitor, 288
 - command line, 288, 300
 - command line tools, 288
 - custom commands, 288
 - default, 288
 - device ping, 288
 - disk thresholds, 288
 - license manager, 288
 - licensing, 288
 - managing tools, 288
 - OpenSSH, 288
 - ping, 335
 - PMP, 288
 - program launch, 288
 - program launch tools, 288
 - ProLiant Support Pack, 288
 - property pages, 288
 - replicate agent settings, 288
 - Resource Process Manager, 288
 - script launch tools, 288
 - Serviceguard clusters, 288
 - system information, 288
 - system page, 288
 - system type manager, 102, 104
 - update system software, 288
 - using, 288
 - version control, 288
 - VMM, 288
 - WBEM, 442
 - trademarks, 32
 - transitioning
 - Transitioning to HP SIM, 66
 - trap, 232
 - details, 232
 - tree controls, 175
 - tree view, 199
 - troubleshooting, 66, 601
 - trust relationship, 142
 - CMS, 46
 - trusted certificate, 163
 - deleting, 166
 - exporting, 165
 - importing, 164
 - require, 167
 - trusted certificates
 - deleting, 163
 - exporting, 163
 - importing, 163
- ## U
- understanding
 - Understanding security, 66
 - uninstalling
 - RPM Package Manager, 378–379
 - UNIX
 - commands, 306
 - unknown, 81
 - unmanaged, 81
 - unregistering
 - MIB, 366
 - VM host, 440
 - Unsubscribe to WBEM Events, 445
 - unsubscribing
 - WBEM events, 504, 528
 - WBEM indications, 526
 - updating

- authorizations, 132, 136
 - upgrading, 36
 - HP 9000 iLO firmware, 360
 - HP Integrity firmware, 360
 - UPS, 81
 - user groups, 119, 132
 - adding, 119
 - administering, 115
 - deleting, 124
 - editing, 121
 - report, 125
 - user rights, 114
 - user settings, 50
 - user templates, 117
 - default, 126
 - user-template, 126
 - users, 117, 132
 - administering, 115
 - authorizing, 133
 - creating, 52, 117
 - deleting, 124
 - editing, 121
 - overview, 115
 - report, 125
- V**
- VCRM catalog problems, 601
 - verifying
 - RPM Package Manager, 378, 380
 - version control, 36, 419–426, 428
 - overview, 418
 - version control agent, 192
 - version control repository
 - selecting, 566
 - version numbers
 - mxtool, 303, 305–306, 333
 - viewing
 - audit log, 597
 - cluster CPU utilization, 298
 - data collection task results, 558
 - license database contents, 346
 - license details, 349
 - MIB list, 361, 365
 - scheduled tasks, 281
 - System Overview page, 178
 - task, 281
 - task configuration, 518
 - task instance, 281
 - task results, 276–277, 281, 284, 519, 522, 535, 537
 - viewing definition
 - automatic event handling tasks, 509
 - views, 500
 - virtual machine, 288
 - launching remote console, 391
 - management, 437
 - virtual machine guest
 - identity tab, 390
 - pausing, 394
 - resetting, 393
 - starting, 392
 - stopping, 395
 - VM performance tab, 397
 - virtual machine host
 - identity tab, 388
 - VM performance tab, 396
 - virtual machine issues, 601
 - VM
 - status, 441
 - VM Host, 438, 440
 - VM host, 437, 441
 - registering, 440
 - unregistering, 440
 - upgrading, 441
 - VM performance tab
 - VM guest, 397
 - VM host, 396
 - VM server, 36
 - VMM, 36, 437–438, 440–441 (see HP ProLiant Essentials Virtual Machine Management Pack)
 - VMM Windows agent
 - deploying, 438
 - VMware ESX, 437
 - VPM, 36, 192
- W**
- Wake on LAN, 377
 - warranty, 32
 - WBEM, 50, 101, 338, 383, 387, 458, 548, 555, 568 (see Web-Based Enterprise Management)
 - status, 212
 - tools, 442
 - WBEM indications, 36
 - HP-UX systems, 36
 - Linux systems, 36
 - port, 526
 - SMI-S systems, 36
 - subscribing, 526–527
 - subscribing to, 504
 - unsubscribing, 526, 528
 - unsubscribing to, 504
 - WBEM property pages, 36
 - WBEM Providers for Linux
 - accessing, 444
 - overview, 444
 - WBEM Settings, 550–551

- Web JetAdmin, 446
- web launch tools, 301, 326
 - creating, 333
 - parameters, 325
- Web-Based Enterprise Management, 338
- Web-Based Enterprise Services, 446, 530
- Web-launch aware tools, 306
- WEBES (see Web-Based Enterprise Services)
- Webmin, 459
 - accessing, 459
- what's new, 41
- Windows, 438, 599
 - configuring locale, 58
 - viewing MIB list, 361
- Windows NT event log, 601
- Windows NT Event Log problems, 601
- Windows XP Service Pack 2, 601
- WLA (see Web-launch aware tools)
- WMI Mapper proxy, 555
 - adding, 544–545
 - deleting, 208, 544, 546
 - editing, 544–545
 - overview, 544
- WMI Mapper problems, 601
- Workload Manager , 446
 - overview, 460
- workstation, 81

X

- X application tool, 301
- X clients , 58
- X Resource file properties , 58
- X window tool
 - creating, 305
- xlsfonts, 58