

Symantec™ IT Management Suite 8.5 powered by Altiris™ technology Administration Guide



Symantec™ IT Management Suite 8.5 powered by Altiris™ technology Administration Guide

Legal Notice

Copyright © 2019 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and Altiris are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<https://www.symantec.com>

Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

Knowledge Base Articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

<https://support.symantec.com>

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

<https://www.symantec.com/connect>

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:

<https://entced.symantec.com/default/ent/supportref>

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Section 2	Configuring the Symantec Management Platform	44
Chapter 4	Configuring Notification Server	45
	About Notification Server	45
	About configuring Notification Server	46
	Configuring Notification Server settings	47
	Notification Server processing settings	49
	Mail server and address settings	50
	Status message logging settings	51
	Opening the Log Viewer	52
	Proxy server settings	52
	Distribution point credential settings	53
	Manually synchronizing the KMS encryption keys	53
	Backing up critical Notification Server data	54
	Configuring Notification Server settings with NS Configurator	55
	Viewing the settings of the Configuration Management Database	56
	Purging the Configuration Management Database	58
	Saving resource data history in the CMDB	60
Chapter 5	Configuring security	61
	About Symantec Management Platform security	61
	Setting up Symantec Management Platform security	62
	Creating and configuring security roles	65
	Assigning privileges to a security role	69
	Creating and configuring Symantec Management Platform user accounts	191
	Specifying general Symantec Management Platform user account details	73
	Configuring credentials for a Symantec Management Platform user account	74
	Adding members to a security role	75
	Assigning a Symantec Management Platform user account to a security role	76
	Adding security roles as members of other security roles	77
	Assigning security permissions to folders and items	78
	Customizing permission inheritance	79
	Predefined security roles	80
	Symantec Management Platform security management tasks	82
	Configuring password complexity and lockout settings	83
	Unlocking locked out credentials	85

	Accessing the Security Role Manager	86
	Taking ownership of a folder or item	87
	Managing credentials	88
Chapter 6	Configuring schedules	89
	How Symantec Management Platform uses schedules	89
	Components of a Symantec Management Platform schedule	91
	Managing shared schedules	93
	Configuring a schedule	94
	Viewing the Notification Server internal schedule calendar	95
Chapter 7	Configuring sites and site servers	97
	About site services	97
	About site maintenance	98
	Managing sites	99
	Managing manually assigned agents	101
	Configuring site settings	101
	Managing subnets	103
	Managing site servers	106
	Assigning a site server to a site manually	108
	Configuring global site server settings	109
	Configuring individual connection settings for a site server	110
	Configuring a site server communication profile	112
	About configuring the site service settings	112
	Configuring package service settings	113
	Configuring individual package service settings	113
	Configuring task service settings	114
Chapter 8	Configuring Package Server for Linux	115
	About package server for Linux	115
	About integrating Apache Web Server with package server for Linux	116
	About detecting the Apache Web Server	117
	Requirements to configure package server and the Apache Web Server	118
	Requirements to configure HTTPS and HTTP	120
	Package server configuration example that uses main web directory for package server links	121
	Package server configuration example using an alias for package server links	123

Chapter 9	Configuring hierarchy and hierarchy replication	127
	About Notification Server hierarchy	127
	Hierarchy and replication requirements	128
	Implementing Notification Server hierarchy	129
	Creating and managing hierarchical relationships	130
	Setting up a hierarchical relationship between two Notification Server computers	133
	Configuring hierarchy replication rules	134
	Setting up custom hierarchy replication	137
	Viewing replication progress report	138
	Overriding the hierarchy differential replication schedule	139
	Replicating selected data manually	140
	Setting up a hierarchy automation policy	140
	Running a hierarchy report	141
	Updating summary data	142
Chapter 10	Configuring standalone replication rules	143
	About standalone replication rules	143
	Configuring standalone replication rules	144
	Managing replication servers	146
Chapter 11	Enabling persistent connection	147
	About the Symantec Management Agent communication using persistent connection	147
	Enabling persistent connection in your environment	148
Chapter 12	Configuring Symantec Endpoint Management Workspaces	151
	Preparing Symantec Endpoint Management Workspaces for usage	151
	Configuring access to Symantec Endpoint Management Workspaces	153
	Configuring search scope for endpoints in Endpoint Management Workspaces	154
	Configuring access to Targets in Endpoint Management Workspaces	155
	Setting up the Deliver Software quick task	156
	Setting up the Run Task quick task	157
	Setting up the Reports quick task	158

	Setting up the Change Asset Status quick task	159
Section 3	Discovering the resources in your network	161
Chapter 13	Discovering Windows computers	162
	Resource discovery methods	162
	Discovery methods for Windows computers	163
	Discovering computers with domain resource discovery	164
Chapter 14	Importing resources from Active Directory	168
	About Microsoft Active Directory Import	168
	About importing resource associations	169
	Importing resources using Microsoft Active Directory Import	170
	Creating and modifying resource import rules	171
	Scheduling resource import rules	173
	Configuring the Directory Synchronization schedule	175
	Running resource import rules manually	176
Chapter 15	Discovering network devices	177
	About Network Discovery	177
	Discovering network devices	178
	Configuring discovery settings	179
	Creating Network Discovery tasks using the wizard	180
	Manually creating and modifying Network Discovery tasks	181
	Creating connection profiles with Network Discovery	182
	Creating or cloning a connection profile	183
	Methods for discovering network devices	184
	About selecting network ranges to discover	185
	Viewing discovered devices in organizational views	186
	Viewing discovery reports	187
	Classifying SNMP devices	187
	Delegating Network Discovery tasks to non-administrator users	188
	Adding non-administrator users to security roles for performing Network Discovery tasks	191
	Enabling non-administrator roles to create or run Network Discovery tasks	192
	Granting non-administrator roles privileges to create credentials and connection profiles	195

	Granting non-administrator roles access to the default connection profile	196
	Enabling roles other than predefined security roles to create and run tasks using the Network Discovery wizard	196
	Making a connection profile read-only	198
	Importing MIB files	199
Section 4	Installing and configuring the Symantec Management Agent	200
Chapter 16	Introducing the Symantec Management Agent	201
	About the Symantec Management Agent	201
	Opening the Symantec Management Agent user interface	202
	Enabling the Diagnostics mode in Symantec Management Agent	202
Chapter 17	Installing the Symantec Management Agent on client computers	204
	Methods for installing the Symantec Management Agent	204
	Installing the Symantec Management Agent on Windows computers	206
	Symantec Management Agent for Windows installation prerequisites	208
	Creating an agent registration policy	209
	Specifying the Symantec Management Agent for Windows installation settings	210
	Installing the Symantec Management Agent for Windows with a manual push	211
	Installing the Symantec Management Agent for Windows with a manual pull	213
	Performing a scheduled installation of the Symantec Management Agent for Windows	214
	Viewing the installation status report	215
	Viewing and managing the agent registration status	216
	Installing the Symantec Management Agent on UNIX, Linux, and Mac computers	219
	Creating a CSV file for importing UNIX, Linux, and Mac computers	220
	Symantec Management Agent for UNIX, Linux, and Mac installation prerequisites	221
	Specifying the Symantec Management Agent for UNIX, Linux, and Mac installation settings	222

	Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual push	223
	Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual pull	226
Chapter 18	Upgrading and uninstalling the Symantec Management Agent	228
	Methods for upgrading the Symantec Management Agent	228
	Methods for uninstalling the Symantec Management Agent	229
	Configuring the Symantec Management Agent Upgrade and Uninstall policies	230
	Configuring the Symantec Management Agent package	233
	Removing the Symantec Management Agent for Windows manually	233
Chapter 19	Configuring the Symantec Management Agent	235
	Configuring the Symantec Management Agent using the configuration policies	235
	Configuring the global agent settings	236
	Configuring the targeted agent settings	237
	Configuring the settings for peer-to-peer downloading	239
	Configuring maintenance window policies	244
	Configuring a Notification Server communication profile	247
	Redirecting the Symantec Management Agent to communicate with a different Notification Server	248
Section 5	Implementing Cloud-enabled Management	251
Chapter 20	Introducing Cloud-enabled Management	252
	About Cloud-enabled Management	252
Chapter 21	Preparing your environment for Cloud-enabled Management	254
	Preparing your environment for Cloud-enabled Management	254

Chapter 22	Setting up Cloud-enabled Management	256
	Setting up Cloud-enabled Management	256
	Configuring the Cloud-enabled Management Agent IIS Website Settings	258
	About preparing the Internet gateway computer	260
	Downloading and running the Internet gateway installation package	261
	Configuring the Internet gateway	262
	Enabling the Internet gateway status reporting	264
	Configuring sites and site servers to serve cloud-enabled agents	265
	Configuring the Cloud-enabled Management Settings policy	267
	Generating and installing the Cloud-enabled Management offline package	269
Chapter 23	Performing Cloud-enabled Management tasks	272
	Cloud-enabled Management troubleshooting and maintenance tasks	272
	Managing certificates	273
	Restoring Cloud-enabled Management communication after an off-box upgrade	276
	Revoking a Cloud-enabled Management certificate	278
	Viewing the site server certificates	280
	Forcing the Symantec Management Agent to use a specified Internet gateway	281
	Backing up and restoring an Internet gateway	282
	Viewing Cloud-enabled Management reports	284
Section 6	Managing Symantec Management Platform resources	285
Chapter 24	Configuring resource security	286
	Configuring resource security	286
	Creating and configuring an organizational view	288
	Creating and populating an organizational view or group	289
	Creating and configuring an organizational group	290
	Viewing resources in an organizational group	291
	Setting security on an organizational group	292
	Considerations for resource scoping	293

Chapter 25	Configuring resource filters and targets	297
	About resource filters	297
	Creating or modifying a filter	298
	Creating a new filter in ITMS Management Views	300
	Adding an SQL query to the filter in ITMS Management Views	302
	Adding explicit criteria to the filter in ITMS Management Views	302
	Modifying an existing filter in ITMS Management Views	303
	Creating a new filter in the default filter tree	304
	Selecting the filter query type	305
	Defining a resource query for a filter	306
	Defining an SQL query for a filter	307
	Specifying filter inclusions and exclusions	308
	Modifying an existing filter	309
	Updating the membership of a filter	310
	Saving the filter data in a file	311
	Viewing filter dependencies	311
	About resource targets	312
	Creating a new target in ITMS Management Views	314
	Scheduling resource membership updates	315
Chapter 26	Configuring packages	317
	Editing the configuration settings for a package	317
	Updating the distribution points for a package	318
	Enabling access to a package at a UNC source location	318
Chapter 27	Using policies	319
	About Symantec Management Platform policies	319
	About user-based policies	320
	Managing Symantec Management Platform policies	321
	Pushing a policy in real time	321
	Specifying the targets of a policy or task	322
	Creating or modifying a resource target	323
	Specifying filtering rules for resource target	324
	Specifying a policy schedule	326
	About automation policies	327
	Key components of automation policies	328
	Managing automation policies	330
	Creating or modifying scheduled automation policies	331
	Creating or modifying message-based automation policies	333

	Specifying the automation policy data source	334
	Specifying the automation policy action	336
	Creating and modifying automation policy tasks	337
	Disabling or limiting Notification Server Event processing for a client computer	339
Chapter 28	Using tasks and jobs	340
	About Task Management	340
	Task Management components	341
	How task server uses the tickle mechanism	343
	When to use tasks, jobs, and policies	345
	About running tasks in hierarchy	345
	Sequencing tasks	347
	Deploying a task server	348
	Configuring a Task Server communication profile	349
	Creating a task	350
	Creating a job	350
	Running a job or task	352
	Rerunning a failed task	352
	Adding a schedule to a policy, task, or job	354
	Viewing the task status on the Symantec Management Agent	355
	Viewing and editing permissions on a task type	355
	Creating tasks to input or to output task properties	356
	Cleaning up task data	357
	Cleaning up task schedules	359
	Cleaning up task version data	360
	Changing Client Task Agent settings	360
Chapter 29	Using Resource Manager	362
	About resource management	362
	Accessing Resource Manager	363
	Viewing inventory data for a data class	364
	Viewing event data for a data class	364
	Adding a resource to an organizational group	365
	Resource Manager tasks	365
Chapter 30	Using Notification Server reports	367
	About Notification Server reports	367
	Viewing and managing resource data with Notification Server reports	368

	Extracting Notification Server report results	369
	Viewing Notification Server report results	370
	Using Notification Server report results	371
	Saving Notification Server report results as a file	373
	Creating a static filter from Notification Server report results	373
	Saving Notification Server report results as a snapshot	374
	Saving Notification Server report results as a Web part	375
Chapter 31	Creating custom Notification Server reports	376
	Components of a custom Notification Server report	376
	Creating and modifying custom Notification Server reports	378
	Creating a custom Notification Server report	380
	Modifying an existing custom Notification Server report	381
	Defining a resource query for a custom report	381
	Defining an SQL query for a custom report	382
	Defining parameters and value providers for a custom report	383
	Creating or modifying a chart view for a custom report	385
	Creating or modifying a grid view for a custom report	386
	Setting up drilldown actions for a custom report	387
	Specifying advanced properties of a custom report	389
Chapter 32	Viewing resource information	391
	About resources	391
	Viewing resource data class information	392
	Viewing resource association type information	392
	Viewing resource type information	392
Chapter 33	About Symantec Remote Access Connector	394
	Setting up Symantec Remote Access Connector	394
	Symantec Remote Access Connector configuration file	395
	Creating the Remote Access Connector configuration file template	399
	Importing the Remote Access Connector configuration file	399
	Using a remote connection tool from Symantec Management Console	400
Chapter 34	Configuring Symantec Security Cloud Connector	401
	Setting up Symantec Security Cloud Connector	401

Section 7	Managing CMDB data with Data Connector	404
Chapter 35	Introducing Data Connector	405
	About Data Connector	405
	How Data Connector works	405
	What you can do with Data Connector	406
Chapter 36	Performing data management tasks	408
	Importing and exporting data	408
	About pre-processing data before data imports	409
	Creating a data source definition	410
	Creating a data transfer rule	411
	Creating a resource lookup key	411
	Running a data transfer rule as a task	412
	Viewing data transfer summaries	413
	Checking the health of data transfer rules	413
	Creating a CMDB rule to edit CMDB data	414
	Running a CMDB rule as a task	414
	Creating a virtual data class	415
	Configuring data connector verbose log purging options	416
Appendix A	Security privileges and permissions	417
	Security privilege categories	418
	Security permission categories	420
	Connection Profile privileges	421
	Management privileges	421
	System privileges	423
	Credential privileges	425
	Workflow Directory privileges	426
	Symantec Management Console privileges	426
	Software Management privileges	427
	Right-click Menu privileges	429
	Right-click Menu - Connector Samples privileges	430
	Right-click Menu - Hierarchy privileges	431
	Right-click Menu - Actions privileges	432
	Right-click Menu - Set Asset Status privileges	433
	Resource Management permissions	434
	System permissions	434
	Task Server permissions	435

	Report permissions	435
	Policy permissions	436
	Folder permissions	436
	Filter permissions	436
	Connection Profile permissions	437
	Credential Manager permissions	437
Appendix B	Symantec Management Agent	438
	Recommended Symantec Management Agent data update intervals	438
	Symantec Management Agent for UNIX, Linux, and Mac troubleshooting commands	439
Appendix C	Cloud-enabled Management reference topics	443
	Notification Server command line tools	443
	Ways to configure package servers in a mixed environment	444
	Effects of Cloud-enabled Management on site server functionality	445
	Internet gateway management scripts	447
	About Internet gateway load balancing	447
	Cloud-enabled agent installation package parameters	448
	Cloud-enabled agent installation package for Mac computer	450
	Command line switches for Windows cloud-enabled agent configuration	451
Appendix D	Scriptable fields for modifying Resource Import Export and CMDB rules	453
	Scriptable fields for modifying Resource Import Export and CMDB rules	453
	Expression syntax	454
	Expression operators	454
	User-defined values	455
	String operators	455
	Wildcard characters	455
	Aggregate Types	455
	Expression functions	456
	IT Management Suite glossary	460
	Index	467

Introducing the key components of the IT Management Suite

- [Chapter 1. Introducing the Symantec Management Platform](#)
- [Chapter 2. Introducing the Symantec Management Console](#)
- [Chapter 3. Introducing the Symantec Endpoint Management Workspaces](#)

Introducing the Symantec Management Platform

This chapter includes the following topics:

- [About the Symantec Management Platform](#)
- [Components of the Symantec Management Platform](#)
- [About adding products to the platform](#)
- [Where to get more information](#)

About the Symantec Management Platform

Note: Current documentation applies to the most recent version of the product.

The Symantec Management Platform provides a set of services that IT-related solutions can leverage. Solutions plug into the platform and take advantage of the platform services, such as security, reporting, communications, package deployment, and Configuration Management Database (CMDB) data. Because solutions share the same platform, they can share platform services as well as data. Shared data is more useful than data that is only available to a single solution. For example, one solution collects data about the software that is installed on company computers and another solution uses the data to manage software licenses. A third solution can also use this data to help you update software. This close integration of solutions and the platform makes it easier for you to use the different solutions because they work in a common environment and are administered through a common interface.

The platform provides the following services:

- Role-based security
- Client communications and management

- Execution of scheduled or event-triggered tasks and policies
- Package deployment and installation
- Reporting
- Centralized management through a single, common interface
- Configuration Management Database (CMDB)
- Software Management Framework

When you install a solution or suite, the platform is also installed if it is not already installed.

See [“Components of the Symantec Management Platform”](#) on page 20.

See [“About adding products to the platform”](#) on page 21.

Components of the Symantec Management Platform

Table 1-1 Components of the Symantec Management Platform

Component	Description
Notification Server and Symantec Management Console	<p>The Symantec Management Platform service that processes events, facilitates communications with managed computers, and coordinates the work of the other Symantec Management Platform services. The console is the Notification Server computer's Web-based user interface that lets you manage the platform and its solutions.</p> <p>See “About Notification Server” on page 45.</p> <p>See “About the Symantec Management Console” on page 24.</p>
Configuration Management Database (CMDB)	<p>The database that stores all of the information about managed computers.</p> <p>See “Viewing the settings of the Configuration Management Database” on page 56.</p>
Site servers	<p>The Symantec Management Platform can host several types of middleware components, such as package services, task services, and network boot services. The official name for a middleware component is "site service." Any component that hosts a site service is known as a site server. Site servers can host one or more of these services.</p> <p>See “About site services” on page 97.</p>
Symantec Management Agent	<p>The software that is installed on a computer to enable Notification Server to monitor and manage it. After the Symantec Management Agent is installed, that computer becomes a managed computer.</p> <p>See “About the Symantec Management Agent” on page 201.</p>

Table 1-1 Components of the Symantec Management Platform (*continued*)

Component	Description
Software Management Framework	An interface that lets you create and manage the software resources that are in the Software Catalog. It also lets you manage the packages that are in the Software Library. The Software view provides a central location for initiating the software-related tasks that are performed in your organization.
Reports	A way to gather automated information. You can view reports for any managed computer from the Symantec Management Console. See “Viewing and managing resource data with Notification Server reports” on page 368.

See [“About the Symantec Management Platform”](#) on page 19.

About adding products to the platform

A wide variety of products can run on the Symantec Management Platform. Symantec and other companies provide additional products that run on the platform. For example, Symantec Client Management Suite helps you manage endpoint computers and Symantec Server Management Suite helps you manage servers.

You use Symantec Installation Manager to manage the installation of additional products on the platform. On the Install New Products page of Symantec Installation Manager, you can view a list of available products. You can then easily install and evaluate a product. Products generally have a 30-day evaluator’s license. You can view a list of all of the installed products on the Installed Products page of Symantec Installation Manager.

When you purchase products, Symantec Installation Manager also manages the licenses. On the Product Licensing page, you can apply licenses to installed products and view the status of applied licenses.

For more information, see the *IT Management Suite Installation and Upgrade Guide*.

Where to get more information

Use the following documentation resources to learn about and use this product.

Table 1-2 Documentation resources

Document	Description	Location
<ul style="list-style-type: none"> ■ Release Notes ■ User Guides 	<ul style="list-style-type: none"> ■ Information about new features and important issues. ■ Information about how to use this product, including detailed technical information and instructions for performing common tasks. 	IT Management Suite (ITMS) 8.5 Documentation
Help	<p>Information about how to use this product, including detailed technical information and instructions for performing common tasks.</p> <p>Help is available at the solution level and at the suite level.</p> <p>This information is available in HTML help format.</p>	<p>The Documentation Library, which is available in the Symantec Management Console on the Help menu.</p> <p>Context-sensitive help is available for most screens in the Symantec Management Console.</p> <p>You can open context-sensitive help in the following ways:</p> <ul style="list-style-type: none"> ■ Click the page and then press the F1 key. ■ Use the Context command, which is available in the Symantec Management Console on the Help menu.

In addition to the product documentation, you can use the following resources to learn about Symantec products.

Table 1-3 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	Knowledge Base
Cloud Unified Help System	All available IT Management Suite and solution guides are accessible from this Symantec Unified Help System that is launched on cloud.	Unified Help System

Table 1-3 Symantec product information resources (*continued*)

Resource	Description	Location
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	<p>The links to various groups on Connect are as follows:</p> <ul style="list-style-type: none"> ■ Deployment and Imaging ■ Discovery and Inventory ■ ITMS Administrator ■ Mac Management ■ Monitor Solution and Server Health ■ Patch Management ■ Reporting ■ ServiceDesk and Workflow ■ Software Management ■ Server Management ■ Workspace Virtualization and Streaming

Introducing the Symantec Management Console

This chapter includes the following topics:

- [About the Symantec Management Console](#)
- [Accessing the Symantec Management Console](#)
- [Accessing documentation in the Symantec Management Console](#)
- [Accessing the My Portal page](#)
- [Customizing the Symantec Management Console](#)

About the Symantec Management Console

The Symantec Management Console (usually referred to as "the console") is a Web-based user interface that is the primary tool for interacting with Notification Server and its components, and for managing resources.

The Symantec Management Console is divided into the following areas:

Header

The top portion of the console that includes the following:

- **Menus**, which let you access console pages and dialogs that provide the management functionality for Notification Server. Symantec solutions that are installed on the system may add new items to the menu.
- **Search box**, which lets you search the resource data for the resources that you want. When you perform a search, a search panel appears under where you input the search.
- **A breadcrumb bar** that shows the menu path to the currently displayed page.

Content area	<p>The portion of the console that is below the header can show one of the following:</p> <ul style="list-style-type: none">■ View A view is composed of a tree view and content pane. The tree view, in the left pane, shows a hierarchical arrangement of items that you can select and work with. The content pane, on the right, displays pages based on tree view selections.■ Portal page A portal page displays a collection of different pieces of information that are contained in Web parts. Notification Server includes predefined portal pages, and other portal pages might be included with solutions. You can also create your own portal pages.■ Full page A full page has a single content pane without the treeview.
--------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Some console pages support personalization, which is the ability for a console page to preserve the state of its controls on a per-user basis. For example, one day user A may open a filter page and, to suit their personal preference, re-order the columns in the grid. Meanwhile, user B opens the same page but leaves the grid in its default configuration. The following day, when the users open that filter page, user A sees the page as they configured it on the previous day. User B still sees the default view as they left it on the previous day.

Personalization is currently applied to the reporting pages and filter pages, and to the state of the navigation tree in the view pages. In addition, the My Portal page is personalized for each user.

Accessing the Symantec Management Console

The Symantec Management Console (usually referred to as "the console") can be accessed from the computer that is running Notification Server or remotely. A remote connection requires that the remote computer has access to the Notification Server computer and is running a supported version of Microsoft Windows and Microsoft Internet Explorer. Because the console is Web-browser-based, you do not need to install any special software to use the console.

See ["About the Symantec Management Console"](#) on page 24.

You must be a member of one or more Notification Server security roles to access the console.

See ["About Symantec Management Platform security"](#) on page 61.

Note: The Symantec Management Platform supports NTLM authentication for remote connections. This lets you access the Symantec Management Console from a remote computer without being prompted for a user name and password (sometimes referred to as "single sign-on" to the console). You must be logged on the remote computer with a Symantec Management Platform account, and you should use the fully qualified domain name (FQDN) for the Notification Server name

If you are prompted for a user name and password when you connect to the Symantec Management Console, you may need to add the Notification Server name (FQDN) to the Trusted Sites zone on the remote computer. You can do this through the Control Panel, on the Internet Properties dialog, in the Security tab.

You can also use the smart card authentication to access the Symantec Management Console. For more information about configuring smart card authentication for Symantec Management Console, see the following knowledge base article:

<http://www.symantec.com/docs/DOC9334>

For information about supported browsers, see the Symantec IT Management Suite Platform Support Matrix at the following URL:

<http://www.symantec.com/docs/ HOWTO9965>

Note that Symantec Management Console also requires cookies to be enabled to function properly. If the cookies are disabled, a warning is displayed.

Note: If you experience problems such as console pages showing error messages, data being lost, or UI controls behaving in unexpected ways, check that the name of Notification Server is correctly specified. The Notification Server name may contain only alphanumeric characters. Special characters, including the underscore character, are not allowed.

To access the Symantec Management Console locally

- ◆ On the local computer, on the **Start** menu, click **All Programs > Symantec > Symantec Management Console**.

To access the Symantec Management Console remotely

- 1 On a remote computer, open Internet Explorer, and go to the following URL:

`http://Notification Server Name/altiris/console`

The Notification Server name should be the fully qualified domain name. You can use https if necessary. If the Notification Server is not on port 80, you need to include the appropriate port number after the Notification Server name.

- 2 If you are logged on to the remote computer with an account that is not a Symantec Management Platform account, you are prompted for your user name and password.

If you are logged on to the remote computer with a Symantec Management Platform account, the single sign-on feature handles this automatically. If the prompt appears, you may need to add the Notification Server name (FQDN) to the Trusted Sites zone on the remote computer.

Accessing documentation in the Symantec Management Console

There are two ways you can access documentation within the Symantec Management Console: context-sensitive help and the documentation page. Context-sensitive help lets you access information specific to the location (page, dialog, or tab) you are at within the console. When you access context-sensitive help, the user's guide for the product that is associated with the location opens in a new window with the appropriate topic displayed.

The **IT Management Suite Documentation** page on the Symantec Support Site lets you access user's guides, administration guides, implementation guides, mind maps, and release notes of IT Management Suite and its components.

See ["About the Symantec Management Console"](#) on page 24.

To access context-sensitive help documentation

- 1 In the Symantec Management Console, make sure the location on which you want to access help is active.

To make a location active, click somewhere in the location. For example, click in the page or dialog.

- 2 Do one of the following:
 - On the **Help** menu, click **Context**.
 - Press the **F1** key.

To access the documentation page

- 1 In the Symantec Management Console, on the **Help** menu, click **ITMS Documentation**.
- 2 On the **IT Management Suite Documentation** page, click the link that is associated with the documentation you want to access.

Accessing the My Portal page

The My Portal page is the default page when a new user opens the Symantec Management Console.

Any changes that a user makes to the My Portal page, such as adding, editing, or removing Web parts, is personalized to that user. The changes are saved according to their user ID. When the user next logs on and selects the My Portal page option from the Console menu, their personalized My Portal page is automatically reloaded.

See [“Creating and modifying portal pages”](#) on page 34.

To access the My Portal page

- ◆ In the Symantec Management Console, on the **Home** menu, click **My Portal**.

Customizing the Symantec Management Console

You can customize the Symantec Management Console to suit the requirements of your organization. For example, you may want to add extra submenu items to the console menu to suit the users in your organization. You cannot change the top-level menu options, and you cannot edit or remove any of the submenu items that are supplied with the Symantec Management Console.

Most customizations are system-wide. To achieve role-level customization, you can use security on items. For example, you can create a portal page that is accessible only to a certain role. In this case, customization is implemented with permissions on items, not privileges. Views, trees, and menus can also be customized using security. For example, a Symantec administrator can set the permission on a tree item or menu option so that users in one role can see it, but users in another role cannot. However, the My Portal page and per-page personalization applies per-user.

Table 2-1 Customization tasks

Task	Description
Customize menus	Add submenus and submenu items, and set up the menu structure that best suits your organization. See “Customizing the console menu” on page 29.

Table 2-1 Customization tasks (*continued*)

Task	Description
Customize context menus	Add user-defined actions to the right-click menu. See “Adding user-defined actions to the context menu” on page 30.
Customize views	Create and modify views to set up the navigation tree structure that best suits your organization. See “Creating and modifying views” on page 32. See “Adding new items directly to a view” on page 33.
Customize portal pages	Create and modify portal pages. A portal page is a Symantec Management Console page that you can customize to suit your requirements. You can use a portal page to consolidate key information into a single, easy-to-view page. A portal page can display the status of the Symantec Management Platform and managed computers, or any other information that you want to make available. For example, you can include external web pages, intranet pages, RSS feeds, or your own applications. See “Creating and modifying portal pages” on page 34.
Customize Web parts	Create and modify the Web parts that you use to build portal pages. See “Creating and modifying Web parts” on page 36.

You can save your customized console elements as XML files, and restore them when necessary by importing the appropriate files.

See [“Saving console elements as XML files”](#) on page 37.

Customizing the console menu

You can customize the console menu to suit your requirements. The menu options that are supplied with the Symantec Management Platform are read-only and cannot be modified. You can add new submenus, and can modify them as necessary. You can move or delete any menu item, except those that have been designated as read-only.

See [“Customizing the Symantec Management Console”](#) on page 28.

To customize the console menu

- 1 In the Symantec Management Console, on the **Settings** menu, click **Console > Menus**.
- 2 On the **Edit Menu** page, perform the appropriate customization tasks:

To add menu items	<ol style="list-style-type: none">1 In the left pane, right-click the menu item under which you want to add the new menu item, and then click New Item.2 On the Menu Details page, specify the menu item details, and then click Apply.
To add submenus	<ol style="list-style-type: none">1 In the left pane, right-click the menu item under which you want to add the submenu, and then click New Submenu.2 Click Apply.
To import submenu items from an XML file	<ol style="list-style-type: none">1 In the left pane, right-click the submenu to which you want to import menu items and then click Import Submenu.2 In the Choose the XML File to Import dialog box, select the appropriate XML file, and then click Open.3 Click Apply.
To export a submenu to an XML file	<ol style="list-style-type: none">1 In the left pane, right-click the submenu that you want to export, and then click Export....2 In the Destination File for Exported XML dialog box, specify the XML file name and location, and then click Save.
To import the entire console menu from an XML file	<ol style="list-style-type: none">1 In the left pane, on the toolbar, click the Import entire menu icon.2 In the Choose the XML File to Import dialog box, select the appropriate XML file, and then click Open.

Adding user-defined actions to the context menu

The console context ("right-click") menu contains the menu options that are relevant to the folder or item on which you have clicked. A default set of right-click menu options is provided with the Notification Server, and installed solutions may add further options. Most of the default set of options are common functions that are available to most folders and items.

You can create user-defined actions and make them available in the context menu. The action may be one of the following:

- Open a URL and substitute details of the selected resource into the URL. For example, the resource name.
- Run a command line on the Notification Server computer or the computer on which the browser is running.

Note: Each user that wants to run command line right-click actions on a computer needs to have the appropriate SSL certificate installed on the computer. You can download the SSL certificate that you need from the **Command Line Right-Click Action Certificate** page.

You can specify the resources to which the action applies by selecting the resource type and (optionally) filtering the resources with a query. When you right-click a resource of the appropriate type that meets the filter query (if a filter was specified), the context menu that appears includes the user-defined action.

You require the New Right-Click Action privilege to be able to add a user-defined action to the context menu.

See [“Security privilege categories”](#) on page 418.

To add a user-defined action to the context menu

- 1 In the Symantec Management Console, on the **Settings** menu, click **Console > Right-Click Actions**.
- 2 In the left pane, right-click the folder to which you want to add the right-click action, and then click **New > Right-Click Action**.
- 3 In the **New Right Click Action** page, specify the appropriate name and description.
- 4 Configure the action that you want by making the appropriate settings:

Enable	The action must be enabled to be included in the context menu. The new action is disabled by default, which lets you configure and test the action before you make it available to console users.
Resource Type	The resource type to which the action applies. By default all resources of the specified type are included. If you want to apply the action to a specific subset of resources, you can filter the resources with a suitable query expression.
Action Type	In the drop-down list, select the appropriate action type: <ul style="list-style-type: none">■ URL In the Base URL box, specify the appropriate URL. The URL can be to another page in the Symantec Management Console, or to an external intranet or Internet site.■ Command Line In the Command Line box, specify the appropriate command line. Check the Run At Server check box to run the command line from the server. If you leave this check box unchecked, the command line is run from the computer on which the action is invoked.

Substitution Parameters Substitution parameters let you use a variable in the command line or URL and have the value substituted with the appropriate value at run time. For example, the resource name, IP address, or GUID.

For each substitution parameter that you want to include:

- 1 Click **Add**.
- 2 In the **Select Attributes** window, select the attribute that you want to use as a parameter, and then click **OK**.
- 3 Under **Parameter Name**, type the appropriate name for the parameter.

5 Click **Apply**.

See “[Customizing the Symantec Management Console](#)” on page 28.

Creating and modifying views

Notification Server and solutions include predefined views that you can modify and extend as necessary. You can also create and modify your own views.

To create or modify a view

- 1 In the Symantec Management Console, in the **Settings** menu, click **Console > Views**.
- 2 In the left pane, in the **Views** folder, do one of the following:

To create a new view Right-click the folder to which you want to add the view, and then select **New > View**.

To modify an existing view Right-click the view that you want to modify and then select **Edit View**.

- 3 On the **Edit View** page, specify the appropriate details in the following fields:

Name The view name.

Description A description of the view.

Display portal page Lets you select a portal page to associate with the root folder of the view. When the root folder of the view is selected in the left pane, the specified portal page is displayed in the content pane.

Contents of this view Displays the structure of the view that you are creating, and lets you create new folders and delete any items that you don't want.

The contents are sorted alphabetically, with folders on top, followed by items. You cannot modify the structure.

Available items Displays the Symantec Management Console tree structure, and lets you select the folders and items that you want to include in the view.

To add an item to the view:

- 1 In the **Tree** drop-down list, select the tree from which you want to select items.
- 2 Expand the tree and select the folder or item that you want to add to the view.
- 3 Click **Add**.

- 4 Click **OK**.

Adding new items directly to a view

You can add new folders, item links and Web links directly to a view. You can also add new views to create a hierarchy of views.

To add a new component directly to a view

- 1 In the Symantec Management Console, in the **Settings** menu, click **Console > Views**.
- 2 In the left pane, right-click the folder under which you want to add the new folder or item and select the appropriate option:

New > Folder In the **New Folder** dialog box, type the new folder name, and then click **Apply**.

New > Item Link In the **Edit Item Link** window, select the item to which you want to create an item link, and then click **OK**.

New > Web Link In the **Web Link Configuration** dialog box, specify the URL of the web page to which you want to link.

You can optionally specify the following:

- Icon Image URL
If you want to use an icon in the tree view, specify the URL to the appropriate image file.
- Target Frame
The default is rightPane, which is the main content area usually known as the right pane.

Click **Apply**.

New > View In the **Edit View** window, create the appropriate view.

See [“Creating and modifying views”](#) on page 32.

Creating and modifying portal pages

A portal page is a Symantec Management Console page that you can customize to suit your requirements. You can use a portal page to consolidate key information into a single, easy-to-view page. A portal page can display the status of the Symantec Management Platform and managed computers, or any other information that you want to make available. For example, you can include external Web pages, intranet pages, RSS feeds, or your own applications. This is more convenient than viewing a number of different console pages to gather the information that you want.

See “[Customizing the Symantec Management Console](#)” on page 28.

Most portal pages are available to all console users. The exception is the My Portal page, which is a special portal page that is unique to each user.

See “[Accessing the My Portal page](#)” on page 28.

Note: To view a portal page, you require Read permission on that portal page.

Portal pages are constructed from Web parts. You can create and customize Web parts according to your requirements and then add them to your portal pages.

The types of Web parts are as follows:

Report	Displays the information that is retrieved from a report.
URL	A link to another Web page (such as a page in your corporate intranet, or an external Web site).

Portal pages can be up to three columns wide. Web parts may be displayed on a portal page in three different sizes, depending on which column they are placed in or whether they span all columns. The left and middle columns are the same width (Web parts in these are “small”), and the right column is wider (Web parts here are “large”). Alternatively, a Web part can use the full page width (Web part is “multi-column”). These multi-column Web parts are shown at the top or bottom of the portal page. When you design a new Web part, you need to ensure that it displays appropriately at any size. You cannot set a particular size as a Web part property.

You can collapse a Web part by clicking the arrow at the top right, and expand it by clicking the arrow again. This lets you include slow-to-load or rarely-used Web parts on a portal page.

Portal pages have the following two modes of operation:

View	The portal page is read-only. You can view all the Web parts, but cannot make any changes. Some portal pages that are provided by Symantec solutions may be restricted to view mode to prevent anybody from modifying the content.
------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Edit If you have Write permission on the portal page, you can edit it. You can add, remove, resize, and re-order Web parts on a portal page. The Web parts tree is displayed on the left of the page, letting you drag and drop Web parts to the appropriate locations. To remove a Web part from a portal page, click the X symbol at the top-right corner of the Web part.

See [“Creating and modifying Web parts”](#) on page 36.

To create or modify a portal page

1 In the Symantec Management Console, in the **Settings** menu, click **Console > Portal Pages**.

2 Do one of the following:

To create a new portal page In the left pane, right-click the **Portal Pages** folder, and then select **New > Portal Page**.

To modify an existing portal page In the left pane, in the **Portal Pages** folder, select the page that you want to edit.

In the upper-right corner of the portal page, click **Edit**.

3 On the **Portal Page Configuration** page, specify the page name and description and select the Web parts that you want to use on the portal page.

Name The name of the portal page.

Description A description of the portal page.

Web Parts panel This panel contains the list of available Web parts that you can add to the portal page.

To add a Web part:

1 Select the Web part, and then click **Add**.

2 In the portal page, click the Web part and drag it to the appropriate location on the page.

4 If you want to remove a Web part from the page, in the appropriate Web part frame, click the **Delete** symbol in the upper-right corner.

5 Click **Apply**.

Creating and modifying Web parts

Web parts are mini Web pages that you can use as the building blocks for portal pages. A Web part can display a report or the contents of a Web page. The console is supplied with a set of predefined Web parts that you can use to build your portal pages. You can modify these Web parts, and also create new ones.

See [“Creating and modifying portal pages”](#) on page 34.

You can also create a report Web part directly from a report.

See [“Saving Notification Server report results as a Web part”](#) on page 375.

To create or modify a Web part

1 In the Symantec Management Console, in the **Settings** menu, click **Console > Web Parts**.

2 Do one of the following:

To create a new Web part In the left pane, expand the **Web Parts** folder, and right-click the folder in which you want to add the new Web part.

Click **New > Web Part**.

To modify an existing Web part In the left pane, expand the Web Parts folder, and select the Web part that you want to modify.

3 On the **Web Part Configuration** page, specify the Web part parameters:

Name The name of the Web part.

Description A description of the Web part.

Web Part Contents The content of the Web part. You can choose one of the following:

- Results from report

If you choose this option, you need to select the appropriate report.

The report is run when you open a portal page that contains the Web part, so the results are always up-to-date.

- Show URL

If you choose this option, specify the appropriate URL.

Fixed Height Check this option to specify a fixed height for the Web part, and then type the height (in pixels) in the adjacent box.

If this option is not selected, the Web part resizes according to the content that it displays.

Default size

The default size of the Web part:

- Small
- Large
- Multi-column

When the Web part is added to a portal page, its default location is determined by its default size. If you move the Web part to another location it is resized automatically.

- 4 If you want to cancel the changes without saving anything, click **Cancel**.
- 5 Click **Save Changes**.
- 6 If you want to preview the Web part that you have specified, click **Show Preview**.

Saving console elements as XML files

You can save console elements (menu items, views, portal pages, or Web parts) as XML files. You may want to do this to create backup files before you customize the console. You could also do this to create XML files that you can customize and import as custom console elements into other Notification Servers.

See [“Customizing the Symantec Management Console”](#) on page 28.

To restore console elements, you import them from the appropriate XML files. Console elements are identified by their GUIDs. Elements in the imported XML file overwrite the existing elements that have matching GUIDs. Any elements in the XML that don't have matching GUIDs in the console are added as new items.

Note: You need the Import XML privilege to import XML files. By default, only the Symantec Administrator role has this privilege.

To save a console element as an XML file

- 1 In the Symantec Management Console, in the left pane, click the tree node that you want to save.
- 2 Right-click, and then click **Export**.
- 3 In the **Destination File for Exported XML** dialog box, specify the XML file name and location, and then click **Save**.

To restore a console element from an XML file

- 1 In the Symantec Management Console, in the left pane, select the folder to which you want to restore the element.
- 2 Right-click, and then click **Import**.

- 3 In the **Choose the XML File to Import** dialog box, select the appropriate XML file.
- 4 If you want to prevent any changes from being made to the imported element, check **Open as read-only**.
- 5 Click **Open**.

Introducing the Symantec Endpoint Management Workspaces

This chapter includes the following topics:

- [About Symantec Endpoint Management Workspaces](#)
- [Accessing Symantec Endpoint Management Workspaces](#)
- [About Time Critical Management](#)

About Symantec Endpoint Management Workspaces

Symantec Endpoint Management Workspaces is a console with dedicated pages (workspaces) and widgets that are designed to simplify and speed up the day-to-day endpoint management jobs. With the help of the Symantec Endpoint Management Workspaces, the help desk workers can respond quickly to tickets and requests.

The Symantec Endpoint Management Workspaces are divided into the following areas:

Header

The top portion of the console that includes the following:

- A menu, which lets you access the **Help Center** and change the language of the Symantec Endpoint Management Workspaces. Also, in the menu, you can see the name of the user who is currently signed in.

Navigation bar	<p>The vertical left side portion of the console that includes the following:</p> <ul style="list-style-type: none"> ■ Search The view is composed of a search bar and available resources list. You can search for resources by entering a name or type and view details for a selected resource. ■ Workspaces After you click the Workspaces icon, a fly-out panel appears and displays available workspaces. <p>Note: In Symantec IT Management Suite 8.5, two workspaces are available - Quick Tasks and Time Critical Management. Note that by default, the Time Critical Management workspace is only available to Symantec Administrators role and Symantec Supervisors role.</p> <p>See “About Time Critical Management” on page 41.</p> <p>Click on one of the workspaces to view available widgets for selected workspace.</p>
Content area	<p>The portion of the console below the header that can show one of the following:</p> <ul style="list-style-type: none"> ■ Workspace area ■ Wizard <p>Depending on the widget or workspace that you click, you may view a workspace area dedicated to that widget or a wizard that helps you perform a task. For example, if you click the Deliver Software widget, a Software Delivery wizard opens and helps you perform software delivery to one or more endpoints.</p>

Specifically for help desk workers, Symantec introduces a new out-of-the-box role - **Endpoint Management Workspaces Users**. The role is created to simplify access management to the Symantec Endpoint Management Workspaces for help desk users.

By default, the **Endpoint Management Workspaces Users** role gives the permission to the user to perform the following actions in the Symantec Endpoint Management Workspaces:

- Search for resources.
- View selected resource details.
- Use **Quick Tasks** workspace.

Note: By default the **Endpoint Management Workspaces Users** role does not give the permission to view and use the **Time Critical Management** workspace in Symantec Endpoint Management Workspaces.

See [“About Time Critical Management”](#) on page 41.

For information about how to use the Endpoint Management Workspaces, see the Endpoint Management Workspaces [online help](#).

Before the users with the **Endpoint Management Workspaces Users** role can perform any actions in the Symantec Endpoint Management Workspaces, you need to prepare the role, assign appropriate permissions and set up the quick tasks.

See [“Preparing Symantec Endpoint Management Workspaces for usage”](#) on page 151.

Accessing Symantec Endpoint Management Workspaces

Symantec Endpoint Management Workspaces is a console with dedicated pages (workspaces) and widgets that are designed to simplify and speed up the day-to-day endpoint management jobs. With the help of the Symantec Endpoint Management Workspaces, the help desk workers can respond quickly to tickets and requests.

To access the Symantec Endpoint Management Workspaces from the Symantec Management Console

- ◆ In the Symantec Management Console, on the **Home** menu, click **Endpoint Management Workspaces**.

To access the Symantec Endpoint Management Workspaces remotely

- 1 On a computer, open Internet Explorer, and go to the following URL:
`http://Notification Server Name/altiris/workspaces`
- 2 If you are logged on to the remote computer with an account that is not a Symantec Management Platform account, you are prompted for your user name and password.

See [“About Symantec Endpoint Management Workspaces”](#) on page 39.

About Time Critical Management

The Time Critical Management workspace lets you gather inventory on endpoints in real time so that you can perform immediate hardware and software state analysis. You can also perform various actions on endpoints in real time.

To allow receiving the inventory data and running tasks on endpoints in real time, persistent connection is implemented and used for communication between Notification Server and endpoints. Persistent connection also allows real time communication with the endpoints that are outside of the internal corporate network and use Cloud-enabled Management (CEM) to communicate with Notification Server.

See [“About the Symantec Management Agent communication using persistent connection”](#) on page 147.

Depending on the Time Critical Management task, you can perform it either in the Time Critical Management workspace or in the Symantec Management Console.

Table 3-1 Time Critical Management tasks

Task	Portal	Description
Verify that the inventory data is up-to-date.	Time Critical Management	On the Time Critical Management page, you can search for data classes for which you want to verify that the data is up-to-date. If the data is older than you require, you can immediately update it.
Run tasks in real time.	Time Critical Management	After you find the data classes that you require, you can then select endpoints on which you want to perform further actions. For example, you can run a specific task on selected systems.
Deploy patches or software packages.	Time Critical Management	You can deploy patches or software to the endpoints in real time. This feature is available starting from IT Management Suite 8.5 RU1.
Organize and manage data.	Time Critical Management	You can save selected endpoints as a target or a CSV file, or send the results in an email.
Immediately push policies to the endpoints.	Symantec Management Console	You can select any policy and push it immediately to the required endpoints. Note that the policy is immediately delivered to the endpoints, but it runs according to the specified schedule. See “Pushing a policy in real time” on page 321.

To open the Time Critical Management workspace, use the menu in the Symantec Management Console or enter the Symantec Endpoint Management Workspaces URL in the web browser.

See [“Accessing Symantec Endpoint Management Workspaces”](#) on page 41.

By default, the Time Critical Management workspace is available for **Symantec Administrators** role and **Symantec Supervisors** role.

Note: In the hierarchy, you can perform tasks in real time only on the endpoints that Notification Server manages directly. On parent Notification Server, the endpoints of a child Notification Server are always considered as having non-persistent connection.

If on parent Notification Server, in the Time Critical Management workspace, you start an update inventory task for the endpoints of child Notification Server, the task does not run on these endpoints immediately. Instead, the task instance is replicated down to child Notification Server and then the child Notification Server starts the update inventory task for its endpoints.

Configuring the Symantec Management Platform

- [Chapter 4. Configuring Notification Server](#)
- [Chapter 5. Configuring security](#)
- [Chapter 6. Configuring schedules](#)
- [Chapter 7. Configuring sites and site servers](#)
- [Chapter 8. Configuring Package Server for Linux](#)
- [Chapter 9. Configuring hierarchy and hierarchy replication](#)
- [Chapter 10. Configuring standalone replication rules](#)
- [Chapter 11. Enabling persistent connection](#)
- [Chapter 12. Configuring Symantec Endpoint Management Workspaces](#)

Configuring Notification Server

This chapter includes the following topics:

- [About Notification Server](#)
- [About configuring Notification Server](#)
- [Configuring Notification Server settings](#)
- [Configuring Notification Server settings with NS Configurator](#)
- [Viewing the settings of the Configuration Management Database](#)
- [Purging the Configuration Management Database](#)
- [Saving resource data history in the CMDB](#)

About Notification Server

Notification Server is the primary server component within the Symantec Management Platform. Notification Server coordinates the various solutions and provides the primary user interface, policy-based administration, reporting, and notification. Notification Server hosts the Web-based management console that lets you manage the components of your Symantec Management Platform.

See [“Components of the Symantec Management Platform”](#) on page 20.

See [“About configuring Notification Server”](#) on page 46.

Notification Server is responsible for managing the predefined policies and tasks that are available in each installed solution. These policies and tasks activate components of Notification Server that process several functions.

Notification Server functions include the following:

- Discovering resources on the network
- Installing and configuring the management agent on the endpoints
- Collecting client-reported information and storing it in the CMDB
- Generating detailed Web Reports
- Sending policy information to the endpoints
- Distributing software packages

About configuring Notification Server

The default Notification Server configuration settings are suitable for most purposes and you do not normally need to change them. These default settings are specified when you install the Symantec Management Platform. However, as the needs of your organization change, you can make the appropriate configuration changes.

See [“About Notification Server”](#) on page 45.

Table 4-1 Types of configurations

Configuration	Description
Configure the Configuration Management Database (CMDB) settings.	See “Viewing the settings of the Configuration Management Database” on page 56. Note: Starting from IT Management Suite version 8.1, you can edit the Configuration Management Database settings in the Symantec Installation Manager.
Set up database purging.	See “Purging the Configuration Management Database” on page 58.
Configure resource data history retention.	See “Saving resource data history in the CMDB” on page 60.
Configure Notification Server settings. These settings include event processing, status message logging, the email message server and default addresses, and a proxy server.	See “Configuring Notification Server settings” on page 47.
Configure the Notification Server settings that do not appear in the Symantec Management Console.	See “Configuring Notification Server settings with NS Configurator” on page 55.
Specify the software delivery package distribution point credentials.	See “Distribution point credential settings” on page 53.

Configuring Notification Server settings

Notification Server settings that you can configure include event processing, status message logging, and the email message server and default addresses.

See [“About configuring Notification Server”](#) on page 46.

You can also configure other Notification Server settings with NS Configurator.

See [“Configuring Notification Server settings with NS Configurator”](#) on page 55.

To configure Notification Server settings

- 1 In the Symantec Management Console, in the **Settings** menu, click **All Settings**.
- 2 In the left pane, under **Settings** folder, expand **Notification Server**, and then click **Notification Server Settings**.

- 3 On the **Notification Server Settings** page, make the appropriate changes on the following tabs:

Processing

You can enable or disable Notification Server Event (NSE) processing and persistent connection on Notification Server. You can also specify the application identity of Notification Server, and restart Notification Server services manually.

See [“Notification Server processing settings”](#) on page 49.

E-mail

You can specify the mail server that Notification Server uses and set the default To and From email addresses.

See [“Mail server and address settings”](#) on page 50.

Logging

You can specify the types of status messages, such as Notification Server errors, warnings and information messages, that you want logged by Notification Server.

See [“Status message logging settings”](#) on page 51.

Proxy

If you don't want to allow Notification Server users direct access to the network, you can configure a proxy server.

See [“Proxy server settings”](#) on page 52.

Distribution Point Credential

You can specify the credentials that Notification Server uses to access your package distribution points.

See [“Distribution point credential settings”](#) on page 53.

Encryption Keys Management

Notification Server uses the encryption keys to protect sensitive data. To allow different Notification Servers to process each other's data, their Key Management Systems (KMS) must be synchronized.

See [“Manually synchronizing the KMS encryption keys”](#) on page 53.

Note that before the standalone or hierarchy replication, the KMS is synchronized automatically.

Critical Data Backup

You can back up KMS encryption keys, certificates, core settings, registry, and Software Library content on demand or at regular intervals.

See [“Backing up critical Notification Server data”](#) on page 54.

- 4 Click **Save changes**.

Notification Server processing settings

On the **Processing** tab, you can enable or disable Notification Server Event (NSE) processing, and specify the application identity of Notification Server. An NSE is an XML file that is passed between Notification Server and the Symantec Management Agent (including solution plug-ins).

See [“Configuring Notification Server settings”](#) on page 47.

Table 4-2 Options on the **Processing** tab

Option	Description
Server Processing	<p>Server processing is enabled by default when you install Notification Server, but there may be occasions when you need to disable or reenale it. For example, when you install a solution, all event processing is automatically paused. After installation completes, event processing should restart automatically. If that does not happen, a warning message appears in the Symantec Management Console, and you are prompted to reenale Notification Server Event (NSE) processing manually. To reenale NSE processing, click on the warning message and then, in the dialog box that appears, click Resume.</p> <p>The NSEs that are received while NSE processing is disabled are stored on the Notification Server computer and are handled after the NSE processing is enabled again.</p> <p>NSEs contain the following information:</p> <ul style="list-style-type: none"> ■ Communication with the Symantec Management Agent ■ Events processing ■ Basic inventory or full inventory ■ Success or failure of package download
Time Critical Management	<p>Under Time Critical Management, you can turn on persistent connection for Notification Server. Persistent connection enables real time data transfer from and to Notification Server and lets you perform tasks on client computers in real time.</p> <p>Note: After you enable the persistent connection for Notification Server, you must also configure and enable persistent connection in Symantec Management Agent communication profiles.</p> <p>See “About the Symantec Management Agent communication using persistent connection” on page 147.</p>

Table 4-2 Options on the **Processing** tab (*continued*)

Option	Description
Application Identity	<p>The application identity of Notification Server is the account under which Notification Server runs. You specify the appropriate user name and password when you install Notification Server, and you only need to update it when necessary. For example, if your organization has a password change policy, the CMDB access credentials may be forced to change. The application identity no longer has permission to log on to the SQL server.</p> <p>Warning: You cannot use special characters in the application identity user name or password. You may use only alphanumeric characters.</p> <p>The user ID that you define requires the following permissions:</p> <ul style="list-style-type: none"> ■ Local administrator permissions on Notification Server and any remote Windows computers to which you want to install the Symantec Management Agent. ■ Permission to act as part of the operating system and log on as a batch job and a service. ■ Permission to log on to the SQL server. <p>If the user ID does not have this permission, you can specify a different user name and password to log on to the CMDB.</p> <ul style="list-style-type: none"> ■ Permission to connect to any SQL server to which Notification Server may attach. <p>For example, an SMS database for Web Administrator for SMS or Lease database for Contract Management Solution.</p> <p>Notification Server services are restarted automatically when the application identity is changed. However, the Restart services option lets you manually restart the services when necessary. For example, if you make a change to the database, you need to restart the services to make the changes take effect.</p> <p>If the application identity password fails, Notification Server is unable to access the CMDB. You cannot reset the application identity through the Symantec Management Console, as the console uses the same password to access Notification Server. You need to use the AexConfig utility to access the Web services directly and reset the application identity password using the appropriate command line.</p>

Mail server and address settings

You can define a mail server and the To and From email addresses for Notification Server email messages. Notification Server uses SMTP to send email messages. The email address can be any valid SMTP address that your SMTP server recognizes. If the **Require SSL** check box is checked, the connection to the SMTP server is encrypted. Note that your SMTP server must support SSL connection.

See [“Configuring Notification Server settings”](#) on page 47.

You can enable Symantec solutions to send you the email messages that are based on the data that Notification Server receives. The email address that you specify can receive notices of reports successfully run, automation actions executed, and system scalability checks. These emails help you monitor and manage your Notification Server activities.

The email settings are configured when you install Notification Server, and you do not normally need to change them. However, if the SMTP server changes, or if you want someone else to receive the email messages, you need to make the appropriate changes.

The **Send Test Email** option lets you test the email server and address settings by sending a message using the current settings. You need to confirm the changes by clicking OK before you send the test email.

Status message logging settings

You can specify the types of status messages, such as Notification Server errors, warnings, and information messages, that you want logged by Notification Server.

By default, the log messages that Notification Server generates are written to log files in the following directories:

- For Notification Server
 ... \ProgramData\Symantec\SMP\Log
- For Symantec Management Agent
 ... \ProgramData\Symantec\Symantec Agent\Log

Note: When you upgrade Notification Server from 6.x to 7.x, the migration wizard writes any messages to the 6.x log file location rather than the 7.x log file location. The 6.x log file location is ... \Program Files\Altiris\Notification Server\Log. You need to look in this log file to see any migration errors. The Log Viewer displays only the logs that are filed at the default 7.x location. The migration log entries are not included.

See [“Configuring Notification Server settings”](#) on page 47.

You can log any of the following message types:

- Errors
- Warnings
- Information
- Trace
- Verbose

You can also choose to archive log files that are older than a particular time. If you set this option, the relevant log files are archived daily at 5:00 A.M.

See [“Opening the Log Viewer”](#) on page 52.

Opening the Log Viewer

Log Viewer lets you monitor several locations of logs for different components like IT Management Suite, Symantec Management Agent, and Symantec Installation Manager. Log Viewer automatically detects whether component is installed to custom location and monitors custom path. Log Viewer lists the real time events, errors, and warnings that occur when performing any action. These messages help you monitor and troubleshoot your Notification Server.

You can use the Log Viewer to determine the problems and their cause. After you identify errors or warnings in the Log Viewer, you can use the error messages to search the Symantec Knowledge Base for the articles that would help you correct the error. You can also raise the issue to the technical support team.

The Log Viewer lets you perform following tasks:

- View error, warning, informational, trace, and verbose messages.
- Search the logs and view the results.
- Bookmark the log items.
- Filter the logs to display a subset of messages.
- Save the filter definitions for later use.
- Perform search in log files without loading them into Log Viewer.

See [“Status message logging settings”](#) on page 51.

To open the Log Viewer

- ◆ On the Notification Server computer, click **Start**, and then click **All Programs > Symantec > Diagnostics > Altiris Log Viewer**.

Proxy server settings

If you don't want Notification Server users to have direct access to the network, you can configure a proxy server. For example, if you have Notification Server and your managed computers inside your organization's firewall, a proxy server provides security. You can set up a proxy server to provide a safe way through the firewall without exposing Notification Server. This setup helps Notification Server safely obtain patches or download solutions from external Web sites.

See [“Configuring Notification Server settings”](#) on page 47.

Using a proxy server may improve Notification Server performance by using less bandwidth and filtering requests when requesting files from the Internet. One example is PMImport data.

The **Test Settings** option validates the proxy server settings by attempting to connect to an external Web site.

If error messages appear when you test the settings, ensure that your authentication credentials are correct. Ensure that your proxy server is running and that no general network errors exist.

Distribution point credential settings

You can specify the distribution point credentials (DPC) that Notification Server uses to access software delivery packages. These packages are located on a network share that is accessed through a UNC path. Notification Server publishes these packages to a virtual HTTP directory that uses the DPC to connect to the UNC share.

See [“Configuring Notification Server settings”](#) on page 47.

You must specify the distribution point credentials before you create a software package that is accessed from an existing UNC path. The credentials must have permission to validate user accounts and have read permission on all the files on the remote distribution points.

Notification Server can use either of the following credentials:

Agent Connectivity Credential All Symantec Management Agents use the Agent Connectivity Credential (ACC) to connect to a secured resource. The ACC is set in the Global Agent Settings policy.

User-specified credentials If the packages are stored in a location that is not accessible with the Agent Connectivity Credential, you can make them accessible. To make packages accessible, specify the user name and password of an account that does have the appropriate access.

You cannot use special characters in the user name or password. You may use only alphanumeric characters.

Manually synchronizing the KMS encryption keys

Notification Server uses the Key Management System (KMS) encryption keys to protect sensitive data. To allow different Notification Servers to process each other's data, their encryption keys must be synchronized.

You can use a standalone replication rule to synchronize the KMS encryption keys, or you can synchronize them manually.

Note that at the beginning of each standalone or hierarchy replication, the KMS encryption keys are synchronized automatically.

To manually synchronize the KMS encryption keys between two Notification Servers

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, under **Settings** folder, expand **Notification Server**, and then click **Notification Server Settings**.
- 3 On the **Notification Server Settings** page, on the **Encryption Keys Management** tab, do the following:
 - On the first Notification Server, export the KMS encryption keys.
To export the KMS encryption keys, click **Export**, type the encryption password, and then click **OK**.
 - On the second Notification Server, import the keys that you exported from the first Notification Server.
To import the KMS encryption keys, click **Import**, choose the XML file to import, type the encryption password, click **OK**, and then click **Save changes**.
 - On the second Notification Server, export the KMS encryption keys.
 - On the first Notification Server, import the keys that you exported from the second Notification Server, and then click **Save changes**.

Note that sometimes you only need to import the KMS encryption keys one way. For example, if you import data from a particular server, you only need the KMS encryption keys of that server.

See [“Configuring Notification Server settings”](#) on page 47.

Backing up critical Notification Server data

You can configure Notification Server to automatically back up critical data that is not stored in Configuration Management Database (CMDB). For example, you can back up Notification Server Web configuration, root certificate, core settings, registry, or Software Library content.

This feature is available starting from IT Management Suite 8.5 RU2.

To back up critical Notification Server data

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, under **Settings** folder, expand **Notification Server**, and then click **Notification Server Settings**.

- 3 On the **Notification Server Settings** page, on the **Critical Data Backup** tab, configure the following settings:

Repository Settings Lets you configure location of the backups and schedule for deleting the outdated backups.

Note: The schedule for deleting outdated backups does not delete the backups that you create in Symantec Installation Manager (SIM).

Notification Server Configuration Backup Lets you create backup manually or configure a schedule for creating backups at regular interval.

Notification Server configuration backup contains its Web configuration, root certificate, core settings, registry, KMS encryption keys, and site server root certificate.

Note that you must turn on the backup schedule if you want it to run automatically. At the upper right of the backup section, click the colored circle, and then click **On**.

Software Library Backup You can back up Software Library content such as software packages and software files data.

Note: This option lets you back up Software Library content only if Software Library is set up on Notification Server. You cannot back up Software Library that is set up on a remote server.

- 4 (Optional) If you want to manually refresh a backup, click **Run now** on the toolbar of the appropriate backup section.
- 5 Click **Save changes**.

See [“Configuring Notification Server settings”](#) on page 47.

Configuring Notification Server settings with NS Configurator

The NS Configurator is a configuration tool that lets you change most core Notification Server configuration settings. You should only use NS Configurator to change these settings if you know the effect that each setting has on the system.

Starting from IT Management Suite 8.5, you can also access and configure the settings in NS Configurator through Symantec Management Console. To access the settings, in the Symantec Management Console, on the **Settings** menu, click **Notification Server > Core Settings**.

See [“About configuring Notification Server”](#) on page 46.

When a user starts NS Configurator, a security check is performed to determine if the user has permission to view or modify Notification Server settings. If a user does not have permission, a warning message appears and the tool closes.

To configure Notification Server settings with NS Configurator

- 1 To start NS Configurator, run the NSConfigurator.exe file.

This file is at `<installation_path>\Altiris\Notification Server\Bin\Tools`.

When you run this tool, it opens the CoreSettings.config file that is at `<installation_path>\ProgramData\Symantec\SMP\Settings`.

- 2 Do one of the following to find the setting you want to change:

- In the navigation tree in the left pane, locate the setting.
- In the search field in the upper right-hand corner, enter your search text and click **Search**. In the list of search results, click the **Show** link for that setting.

- 3 In the right pane, change the setting and click **Save**.

If you enter an invalid value for a setting, an error message appears. You can only save your changes if you enter a valid value.

- 4 To restore the default value, click **Restore Default**.

The **Restore Default** option appears only if the setting had a default value.

Viewing the settings of the Configuration Management Database

Notification Server has a database, called the Configuration Management Database (CMDB). Both Notification Server and solutions use the CMDB to store configuration items and resource data.

Database processing is one of the largest consumers of resources on the Symantec Management Platform. The number of solutions that are installed in your environment and how they are used influences the database requirements. The number of managed computers that report to each Notification Server computer also influences the database requirements.

Each Notification Server computer can be configured to use a local Configuration Management Database (CMDB) or to use a remote CMDB. A Notification Server computer with a local database requires more resources than a Notification Server computer with a remote database configuration.

You can use the following configurations for the CMDB:

Local CMDB configuration	In a local CMDB server configuration, you install the CMDB on the same computer as Notification Server. This configuration is acceptable for the environments that have 1,000 to 5,000 endpoints. In these environments there is minimal contention of resources between Notification Server services and the CMDB services.
Remote CMDB configuration	In a remote CMDB configuration, you install the CMDB on a different computer from the Notification Server computer. This configuration is recommended for most environments. In this configuration the workload of the CMDB is offloaded from the Notification Server computer. The CMDB server and Notification Server computer must have a high-speed network connection between them. Symantec recommends 1GB Ethernet.

You can make any necessary changes to the CMDB configuration settings. When Notification Server is installed, the CMDB is configured as part of the installation process. You do not normally need to make any further changes.

However, there may be occasions when you need to change the CMDB configuration settings. For example, if you upgrade the hardware on which your Microsoft SQL Server runs, or if you are instructed to do so by Symantec Support.

Note: Starting from IT Management Suite version 8.1, you can edit the Configuration Management Database settings in Symantec Installation Manager. For more information about configuring CMDB, see the *Symantec Installation Manager Getting Started Guide*.

To view the settings of the Configuration Management Database

- 1 In the Symantec Management Console, in the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Notification Server**, and then click **Database Settings**.

- 3 On the **Database Settings** page, under **Database Settings**, view the settings of the Configuration Management Database.
- 4 (Optional) Under **Reporting Credentials**, you can edit the credentials that are used for running report queries on the CMDB.

These credentials provide less security than the database credentials (which are for the database administrator). These credentials are used to access the database and run the appropriate SQL query when a user runs a report.

You can use Notification Server application credentials for Windows authentication. You may want to use this method to avoid being affected by any password change policy that is enforced in your organization.

The application credentials are specified in the **Processing** tab of the **Server Settings** page.

See [“Notification Server processing settings”](#) on page 49.

You also have the option to use SQL authentication. To use SQL authentication you can specify the appropriate SQL logon user name and password.

Note: If you want to switch database authentication to SQL, you must change both the **Database Credentials** and the credentials for producing public reports. If you only change the **Database Credentials**, Notification Server is not fully functional, and you may experience errors with some operations.

After you switch the database authentication to SQL, you must click **Validate connection** to check if Notification Server successfully connects to SQL.

To save the changes, click **Save changes**.

Purging the Configuration Management Database

To manage the size of the Configuration Management Database (CMDB), you can specify how long certain types of data are stored. You can specify storage length for data such as reports, managed computers, and event data. For example, if you experience poor performance when running reports, try purging your events or configure the event purging options to save less data.

The data that can be purged from the CMDB includes the following:

- Report snapshots
Snapshots older than a specified amount of time can be deleted.
- The managed computers that have not communicated with Notification Server for longer than a specified amount of time

These can be deleted or set as retired. The CMDB is updated when the CMDB purging schedule is run.

- **Resource event data**

Event data older than a specified amount of time can be deleted. You can optionally specify a maximum number of rows to retain. If the event data table reaches this size, new rows continue to be added until the next scheduled update. When the CMDB purging schedule runs, the table is trimmed back to its maximum size. The table is trimmed by removing the oldest rows, even if the oldest data has not been retained for the specified time.

You can have the same settings for all data classes, or you can set custom settings for some or all data classes. A custom setting for a data class overrides the global setting. If no custom setting is made for a data class, the global setting is used for that data class. The same CMDB purging schedule is used in all cases.

The CMDB purging schedule is a Windows schedule that you set when you install Notification Server. You cannot change it through the Symantec Management Console. If you want to make any changes, you can do so through the Windows Control Panel.

To purge the Configuration Management Database

- 1 In the Symantec Management Console, in the **Settings** menu, click **Notification Server > Purging Maintenance**.
- 2 In the left pane, under **Purging Maintenance** folder, click **Purging Maintenance**.
- 3 On the **Purging Maintenance** page, configure the settings on the following tabs:

Purging Maintenance	Lets you specify the report purge settings, agent registration data, and computer data purge settings. Note that the Purge outdated Agent Registration entries option deletes only items with status Blocked . To override the purging schedule and purge the CMDB immediately, click Purge Now .
----------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Resource Event Data Purge Settings	Lets you specify the resource event data purging settings that you want.
-------------------------------------------	--------------------------------------------------------------------------

Report Data Snapshot Purge Settings	Lets you specify the report data snapshot purging settings. To override the purging schedule and purge the CMDB immediately, click Purge Now .
--------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------

- 4 Click **Save changes**.

Saving resource data history in the CMDB

Notification Server captures resource data in real time as it collects inventory data. You can choose to create a resource data history for each type of resource and resource association. For each history, you can specify how long to retain the history data in the CMDB.

A resource data history can include data from any of the data classes. A resource association history can include data from any of the resource association types.

To save resource data history in the CMDB

- 1 In the Symantec Management Console, in the **Settings** menu, click **Notification Server > Purging Maintenance**.
- 2 In the left pane, under **Purging Maintenance** folder, click **Resource History**.
- 3 On the **Resource History** page, on the **Resource Data History** tab, expand the solution or component, select the data classes for which you want to create resource data history, and then, for each data class, specify the period for which you want to keep the resource data history.

In the corresponding drop-down list, select the time period (**Days, Weeks, or Months**). Then enter the appropriate number of days, weeks, or months.

Any resource data older than the time that is specified for its type is deleted from the CMDB on the purging schedule.

To find the data classes, you can use the filtering option in the upper right corner. You can enter the following values:

string	Displays the data classes that have the entered string in their name.
*	Displays all data classes that have history data.
>x	Displays the data classes that have more than x kB of history data.
=string	Displays the data classes that have the entered string in their history inventory table name in CMDB.

- 4 On the **Resource History** page, on the **Resource Association History** tab, expand the association type, select the associations for which you want to create resource data history, and then, for each association, specify the period for which you want to keep the history.

In the corresponding drop-down list, select the time period (**Days, Weeks, or Months**). Then enter the appropriate number of days, weeks, or months.

Any resource data older than the time that is specified for its type is deleted from the CMDB on the purging schedule.

- 5 Click **Save Changes**.

Configuring security

This chapter includes the following topics:

- [About Symantec Management Platform security](#)
- [Setting up Symantec Management Platform security](#)
- [Symantec Management Platform security management tasks](#)

About Symantec Management Platform security

The Symantec Management Platform uses role-based security, which means that user access is based on the user's security role. A security role is a set of privileges and permissions that is granted to all members of that role. Using role-based security lets you create and maintain a small number of security roles. You can then assign each Symantec Management Platform user account to the appropriate role, rather than assign specific privileges and permissions to each individual user. However, you can also assign specific permissions to individual user accounts.

User accounts, which are sometimes referred to as users, are not the same as user resources in Symantec Management Platform. A user resource is an entity that is used to associate managed devices with the owner of the device. The existing user resources and the user accounts that can log on to the Symantec Management Console or run a workflow are separate entities.

A security role controls user access to the Symantec Management Platform using the following:

- **Privileges**
A privilege applies system-wide. Privileges are assigned only to roles and cannot be assigned directly to individual user accounts. A privilege assigned to a role lets a user account that is a member of that role perform a particular action on the Symantec Management Platform or in the Symantec Management Console. In some cases, the user's role requires the corresponding permissions.
See [“Security privilege categories”](#) on page 418.

- **Permissions on folders and items**
 Permissions specify the access that a security role or user account has to a Symantec Management Console folder or item. A permission on a security role applies to all members of that role. A permission on a folder applies to all of the items that are contained directly in that folder.
 See [“Security permission categories”](#) on page 420.
- **Permissions on organizational views and groups**
 An organizational view is a hierarchical grouping of resources (as organizational groups) that reflects a real-world structure or view of your organization. You can set up resource security by assigning the appropriate permissions for each security role on each organizational view. You also assign the appropriate permissions on the organizational groups within each view. A permission that is assigned to an organizational group applies to all resources in that group. By default, the permission applies to all of its child groups. You cannot assign permissions directly to a particular resource.

Privileges, permissions on folders and items, and permissions on organizational views and groups work together. You need to assign the appropriate combination to each security role to grant user accounts the access that they need to perform their activities.

See [“Setting up Symantec Management Platform security”](#) on page 62.

See [“Symantec Management Platform security management tasks”](#) on page 82.

Setting up Symantec Management Platform security

To give user accounts access to the Symantec Management Platform, installed solutions, and the data that is contained in the CMDB, you need to set up your security roles. You assign the appropriate privileges and permissions to each role. You need to create your Symantec Management Platform user accounts and then add each user account to the appropriate role.

See [“About Symantec Management Platform security”](#) on page 61.

Table 5-1 Process for setting up Symantec Management Platform security

Step	Action	Description
Step 1	Create and configure the security roles that you require.	<p>Security roles control access to the Symantec Management Platform, installed solution functionality, and all the data that is contained in the CMDB.</p> <p>You can create new security roles in the following ways:</p> <ul style="list-style-type: none"> ■ Create new security roles. ■ Clone existing security roles. ■ Import domain groups and users from Active Directory. <p>See “Creating and configuring security roles” on page 65.</p>

Table 5-1 Process for setting up Symantec Management Platform security (*continued*)

Step	Action	Description
Step 2	Assign the appropriate privileges to your security roles.	<p>A privilege allows a role member to perform a particular action on the Symantec Management Platform, or on items in the Symantec Management Console. To perform an action on an item, the role must have the necessary permission on the item.</p> <p>See “Assigning privileges to a security role” on page 69.</p>
Step 3	Create and configure the user accounts that you require.	<p>Each Symantec Management Platform user account contains the credentials that the user needs to access the Symantec Management Console or to run a workflow. The credentials may be internal Symantec Management Platform user names and passwords or Windows accounts.</p> <p>Internal credentials are currently used for workflow integration only. Windows credentials are required to access the Symantec Management Console.</p> <p>You can create new user accounts in the following ways:</p> <ul style="list-style-type: none"> ■ Create completely new user accounts. ■ Clone existing user accounts. ■ Import domain groups and users from Active Directory. <p>See “Creating and configuring Symantec Management Platform user accounts” on page 191.</p> <p>See “Specifying general Symantec Management Platform user account details” on page 73.</p> <p>See “Configuring credentials for a Symantec Management Platform user account” on page 74.</p>
Step 4	Add members to the appropriate security roles.	<p>A user gains access to the Symantec Management Platform, installed solutions, and the data that is contained in the CMDB through their security role membership.</p> <p>You can assign a user to any number of security roles. A user who is a member of multiple security roles has the union of all the privileges and permissions that those roles grant.</p> <p>See “Adding members to a security role” on page 75.</p> <p>See “Assigning a Symantec Management Platform user account to a security role” on page 76.</p> <p>See “Adding security roles as members of other security roles” on page 77.</p>

Table 5-1 Process for setting up Symantec Management Platform security (*continued*)

Step	Action	Description
Step 5	For each security role, assign permissions on the folders and items that are contained in the Symantec Management Console.	<p>Permissions specify the access that each security role has to a Symantec Management Console folder or to a particular item. A permission on an item applies only to the item. A permission on a folder applies to all of the items that are contained directly in that folder. By default, the contents of a folder inherit all the permissions on the folder.</p> <p>See "Assigning security permissions to folders and items" on page 78.</p>
Step 6	(Optional) For each security role, modify the permission inheritance on the Symantec Management Console folder structure.	<p>Modifying permission inheritance lets you customize permissions on the Symantec Management Console folder structure. This means that you can grant a particular permission on a parent folder but remove that permission from some or all of the folder contents.</p> <p>Remember that you configure permissions on folders and the items within those folders. If you configure a folder and grant Write permissions for a particular role, that role has the Write permission to the folder and all its contents. If the folder contains 100 items, and you do not want those items to inherit the Write permission from the parent folder, you can break permission inheritance. In that case, users who are members of the role to which you granted the Write permission have the Write permission on the folder only. However, they do not have the Write permission on the items that the folder contains.</p> <p>The permission inheritance on a folder or item applies to all security roles. You cannot customize permission inheritance per role.</p> <p>See "Customizing permission inheritance" on page 79.</p>

Table 5-1 Process for setting up Symantec Management Platform security (*continued*)

Step	Action	Description
Step 7	(Optional) Configure resource security.	<p>By default, all the predefined security roles have the Read permission on resources.</p> <p>Security-related resources are specially controlled in Symantec Management Platform: Only users who are members of the Symantec Administrators role have full access to security resources by default. Users who are members of the Symantec Supervisors role have Read permissions on security resources by default. No other predefined security role has permissions on any security resources.</p> <p>See “Predefined security roles” on page 80.</p> <p>If you want to restrict or otherwise control access to resources, you can configure resource security. You configure resource security by creating one or more organizational views that model your resource structure. You control access to the resources by assigning permissions to each security role on the appropriate organizational views and groups.</p>

Creating and configuring security roles

A security role is a set of privileges and permissions that is granted to all members of the role. Using role-based security lets you create and maintain a small number of security roles and assign each user account to the appropriate role. You do not need to assign privileges and permissions to each individual user account. You can assign a user account to multiple security roles: a member of multiple security roles has the union of all the privileges and permissions that those roles grant.

See [“About Symantec Management Platform security”](#) on page 61.

Security roles may be nested: a role may be a member of one or more other roles, and its membership may include both roles and user accounts. The only restriction is that you cannot create a circular role membership where a role is a member of itself.

Privileges, permissions on folders and items, and permissions on organizational views and groups work together. You need to assign the appropriate combination to each security role to grant user accounts the access that they need to perform their activities. Privileges can only be assigned to security roles, but permissions may be assigned to security roles and user accounts.

You should decide what security roles to set up based on logical IT worker or user groups in your organization. For example, you might want an IT level 1 worker role, an upper-level management role, and a human resources role. All user accounts in a security role receive

the same privileges and permissions, therefore they have the same level of access to the Symantec Management Platform.

You can create and configure a security role in one of the following ways:

Create a new security role or clone an existing security role. The Symantec Management Platform and some solutions include predefined security roles.

See [“Predefined security roles”](#) on page 80.

If the predefined security roles do not meet the needs of your organization, you can create new roles or clone the existing roles to create new roles. You can then modify the privileges and permissions as appropriate.

See [“To create a new security role or clone an existing security role”](#) on page 66.

Import domain groups and users through Active Directory.

When you import domain groups from Active Directory, a security role is created in the Symantec Management Platform server for the domain group that you want to import. Members of this domain group, including users and subgroups, are also imported. Users are created as accounts, and subgroups are created as roles. The membership relationship is retained during the import.

See [“To import domain groups and users from Active Directory”](#) on page 67.

During Symantec Management Platform installation, the administrator installing the Symantec Management Platform is automatically assigned to the Symantec Administrators role. The administrator can then create any new security roles that are required and assign each role the appropriate privileges and permissions. The administrator can then assign each user to one or more roles.

Symantec recommends setting up the security roles before Notification Server is deployed to your production network.

This task is a step in the process for setting up Symantec Management Platform security.

See [“Setting up Symantec Management Platform security”](#) on page 62.

To create a new security role or clone an existing security role

- 1 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 2 In the left pane, under **Account Management** folder, click **Roles**.

3 On the **Roles** page, in the left pane, take one of the following actions:

- | | |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To create a new role | <p>Click Add.</p> <p>In the New Role dialog box, type the new security role name, and then click OK.</p> <p>The new role appears in the list of roles and the default settings are shown in the right pane.</p> |
| To clone an existing role | <p>Select the security role that you want to clone.</p> <p>Right-click the role, and click Clone.</p> |

4 In the right pane, configure the appropriate settings in the following tabs:

- | | |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Members | <p>The roles and user accounts that are assigned to the role. A role membership may include any number of user accounts and roles. The members of a role have all of the privileges and permissions that the role grants.</p> <p>See “Adding members to a security role” on page 75.</p> |
| Member Of | <p>The security roles to which the role belongs. The role has the union of the permissions and privileges of these roles, combined with any additional permissions and privileges that are assigned directly to the role.</p> <p>See “Adding security roles as members of other security roles” on page 77.</p> |
| Privileges | <p>The privileges that the role grants its members. A privilege lets a user account perform a particular action on the Symantec Management Platform, or on items in the Symantec Management Console. In some cases, the user account must also have a corresponding permission on the item.</p> <p>See “Assigning privileges to a security role” on page 69.</p> |

5 (Optional) If you want to access the Security Role Manager to view or set permissions for the security role, click **Show Security Role Manager Console**.

6 Click **Save changes**.

To import domain groups and users from Active Directory

- 1** In the Symantec Management Console, on the **Actions** menu, click **Discover > Import Microsoft Active Directory**.
- 2** On the **Microsoft Active Directory Import** page, in the description that is labeled **Import Role and Account resources from <data source>, from (none). Perform this import on the specified schedule**, click the user group **(none)**.

- 3 (Optional) Create your own Role and Account import rules.
- 4 In the **Select Security Groups** dialog box, search for the domain groups that you want to add; for example, Administrators and Users.
- 5 Click **Add** to add the selected groups, and then click **OK**.
- 6 Run the rule as a full import to import the selected domain group.
- 7 (Optional) You can also schedule a full import to run at appropriate intervals.

You can use this schedule to synchronize your security role membership with the domain group membership. This means that if you remove a domain user from the domain group, the corresponding Security Account is removed from the corresponding security role. Likewise if you add a domain user to the domain group, the corresponding Security Account is created and added to the corresponding security role. Note that if a domain user is removed from a domain group, the corresponding security account is not deleted. Only the membership to the security role is removed.
- 8 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 9 In the left pane, under **Account Management** folder, click **Roles**, and then click the role that you want to edit.

10 (Optional) In the right pane, configure the appropriate settings under the following tabs:

Members	<p>The roles and user accounts that are assigned to the role. A role membership may include any number of user accounts and roles. The members of a role have all of the privileges and permissions that the role grants.</p> <p>See “Adding members to a security role” on page 75.</p> <p>Note that you should not manually modify members of the roles that you imported from Active Directory. This constraint exists because any subsequent rule executions overwrite the membership configuration.</p> <p>Roles that you import from Active Directory are designed to maintain the same membership as the corresponding domain groups.</p>
Member Of	<p>The security roles to which the role belongs. The role has the union of the permissions and privileges of these roles, combined with any additional permissions and privileges that are assigned directly to the role.</p> <p>See “Adding security roles as members of other security roles” on page 77.</p>
Privileges	<p>The privileges that the role grants its members. A privilege lets a user account perform a particular action on Symantec Management Platform or on items in the Symantec Management Console. In some cases, the user account must also have a corresponding permission on the item.</p> <p>See “Assigning privileges to a security role” on page 69.</p>

11 (Optional) If you want to access the Security Role Manager to view or set permissions for the security role, click **Show Security Role Manager Console**.

12 Click **Save changes**.

Assigning privileges to a security role

You need to specify the privileges that each security role grants to its members. A privilege allows a user to perform a particular action on the Symantec Management Platform, or on items in the Symantec Management Console. To perform an action on an item, the user's role must have the necessary permission on the item. For example, if you give a role the Start Task and Stop Task privileges, you still need to assign the Run Task permission to the role for the appropriate tasks. The role cannot access any tasks that do not have the Run Task permission assigned for that role.

See [“Assigning security permissions to folders and items”](#) on page 78.

Assigning privileges to a security role is part of configuring security roles. This task is a step in the process of setting up Symantec Management Platform security.

See [“Creating and configuring security roles”](#) on page 65.

To assign privileges to a security role

- 1 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 2 In the left pane, click **Account Management > Roles**.
- 3 On the **Roles** page, in the left pane, click the security role that you want to configure.
- 4 In the right pane, on the **Privileges** tab, select the privileges that you want to assign to the role.
To select a privilege, check the corresponding check box.
See [“Security privilege categories”](#) on page 418.
- 5 Click **Save changes**.

Creating and configuring Symantec Management Platform user accounts

Symantec Management Platform has its own user accounts. Earlier than 7.1 versions of Symantec Management Platform used Windows users and groups for user security. Windows users are still used, but they are no longer the only security mechanism.

User accounts, which are sometimes referred to as users, are not the same as user resources in Symantec Management Platform. A user resource is an entity that is used to associate managed devices with the owner of the device. The existing user resources and the user accounts that can log on to the Symantec Management Console or run a workflow are separate entities.

A Symantec Management Platform user account is linked to the Windows credentials that the user requires to access the Symantec Management Console. The user account may also be linked to the internal credentials that it can use to access other Symantec Management Platform services, such as workflows. The user account can be added to the appropriate security roles: an account has the union of all the privileges and permissions that are granted by the roles to which it belongs.

A credential is something that a user account provides to prove its identity. In Symantec Management Platform, a credential may be a user name and password or a Windows account. The user account associates one or more credentials with a particular user and lets the user access the Symantec Management Console or Symantec Management Platform services.

Symantec Management Platform uses two types of credentials:

Internal credential	<p>Lets a user access the appropriate Symantec Management Platform services using a user name and password that is stored in the CMDB. For security reasons, only the hash value of the password is stored.</p> <p>A user account cannot use internal credentials to access the Symantec Management Console. The internal credentials are currently used only for workflow integration.</p>
Windows credential	<p>Lets a user access the Symantec Management Console and Symantec Management Platform services using a Windows user name and password. To use Windows credentials, Notification Server must be in the user's domain, or the user's domain must be trusted by Notification Server domain.</p> <p>You should configure Windows credentials if your organization uses Windows accounts internally. Using Windows credentials lets you enforce password complexity requirements, periodically change passwords, keep password history, and perform other password management tasks in Windows.</p>

You can configure your Symantec Management Platform user accounts to meet the requirements of your organization. You need to create all of the accounts that you want and assign them to the appropriate security roles. Each account has the union of all the privileges and permissions that the roles to which it belongs grants.

You can create and configure a user account in one of the following ways:

- Create a new user account or clone an existing user account.
- Import domain groups and users from Active Directory.

This task is a step in the process for setting up Symantec Management Platform security.

See [“Setting up Symantec Management Platform security”](#) on page 62.

To create a new user account or clone an existing user account

- 1 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 2 In the left pane, click **Account Management > Accounts**.

3 On the **Accounts** page, in the left pane, take one of the following actions:

- | | |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To create a new account | Click Add .

In the New Account dialog box, type the new Symantec Management Platform account name, and then click OK .

The new account appears in the list of accounts. By default, the new account status is Inactive. |
| To clone an existing account | Right-click the Symantec Management Platform account that you want to clone and configure.

Enter the name of the new copy of this account, and click OK . |

4 In the right pane, configure the appropriate settings on the following tabs:

- | | |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General | The general account details. These include the full name and email address of the user for whom the account is created, the account status, and the account credentials.

See “Specifying general Symantec Management Platform user account details” on page 73.

See “Configuring credentials for a Symantec Management Platform user account” on page 74. |
| Member Of | The security roles to which the account belongs. The account has the union of all the privileges and permissions that the roles to which it belongs grants.

See “Assigning a Symantec Management Platform user account to a security role” on page 76. |

5 Click **Save changes**.

To import domain groups and users from Active Directory

- 1** In Symantec Management Console, on the **Actions** menu, click **Discover > Import Microsoft Active Directory**.
- 2** On the **Microsoft Active Directory Import** page, in the description that is labeled **Import Role and Account resources from <data source>, from (none). Perform this import on the specified schedule**, click the user group **(none)**.
- 3** (Optional) Create your own Role and Account import rules.
- 4** In the **Select Security Groups** dialog box, search for the domain groups from which you want to import user accounts; for example, Administrators and Users.
- 5** Click **Add** and then **OK** to add the selected groups.

- 6 Run the rule as a full import to import the selected domain groups.
- 7 (Optional) You can also schedule a full import to run at appropriate intervals.

You can use this schedule to synchronize your security role membership with the domain group membership. This means that if you remove a domain user from the domain group, the corresponding Security Account is removed from the corresponding security role. Likewise if you add a domain user to the domain group, the corresponding Security Account is created and added to the corresponding security role. Note that if a domain user is removed from a domain group, the corresponding security account is not deleted. Only the membership to the security role is removed.

Video: For more information about creating Symantec Management Platform user accounts, see the [Creating a Limited ITMS Administrator Role Video](#) on Symantec Connect.

Specifying general Symantec Management Platform user account details

You need to specify the full name and email address of the user for whom the account is created. You can also change the account status from Inactive to Active when appropriate.

See “[Creating and configuring Symantec Management Platform user accounts](#)” on page 191.

To specify general Symantec Management Platform user account details

- 1 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 2 In the left pane, click **Account Management > Accounts**.
- 3 On the **Accounts** page, in the left pane, click the account that you want to configure.
- 4 In the right pane, on the **General** tab, specify the account details by editing the appropriate boxes:

Full Name	The full name of the user to whom the account belongs.
Email	The email address of the account user.

- 5 (Optional) If you want to activate or deactivate the account, click the status icon in the title bar and then select **Active** or **Inactive**.
- 6 Click **Save changes**.

Configuring credentials for a Symantec Management Platform user account

You need to configure the appropriate credentials to each Symantec Management Platform user account. You can add one Symantec Management Platform internal credential and one Windows credential to a user account. The Windows credential emulates the behavior of previous versions of Symantec Management Platform.

An internal credential lets a user access the appropriate Symantec Management Platform services using a user name and password that is stored in the CMDB. Currently, internal credentials are used only for workflow integration.

A Windows credential lets a user account access the Symantec Management Console and Symantec Management Platform services using a Windows user name and password. To use Windows credentials, Notification Server must be in the user's domain, or the user's domain must be trusted by the Notification Server domain.

You should configure Windows credentials if your organization uses Windows accounts internally. Using Windows credentials lets you enforce password complexity requirements, periodically change passwords, keep password history, and perform other password management tasks in Windows.

See [“Creating and configuring Symantec Management Platform user accounts”](#) on page 191.

To configure credentials for a Symantec Management Platform user account

- 1 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 2 In the left pane, click **Account Management > Accounts**.
- 3 On the **Accounts** page, in the left pane, click the account that you want to configure.

- 4 In the right pane, on the **General** tab, under **Credentials**, click **Add Credential** and then do one of the following:

To add a Windows credential to the account Click **Windows** and then, in the **Windows Credential** dialog box, specify the appropriate Windows user name in Domain/Username format.

If the Windows account is in the same domain as Notification Server, you can omit the Domain and specify the Username only.

If you specify a Windows account that is already assigned to a user account, the Windows credential is removed from the existing account. The Windows credential is then added to the new user account.

To add an internal credential to the account Click **Internal** and then, in the **Create Internal Credential** dialog box, specify the appropriate password.

The password must meet the password complexity settings.

See ["Configuring password complexity and lockout settings"](#) on page 83.

The credential user name is the name of the Symantec Management Platform account and you cannot change it.

- 5 Click **OK**.

The new credential is added to the **Credentials** list.

- 6 (Optional) If you want to modify a credential, select it in the **Credentials** list and then click **Edit**. In the **Edit Windows Credential** dialog box or the **Edit Internal Credential** dialog box, make the appropriate changes and then click **OK**.

For security reasons, the **Edit Internal Credential** dialog box does not display the current password. If you specify a new password, the credential is updated accordingly. If you leave the **Password** box empty, the original password is preserved.

- 7 (Optional) If you want to delete a credential, select it in the **Credentials** list and then click **Delete**.

- 8 Click **Save changes**.

Adding members to a security role

You need to assign the appropriate members—user accounts and other security roles—to each of your security roles. You need to be a member of the Symantec Administrators role or a member of a role that has the Change Security privilege to add members. You can assign a user account to any number of security roles. The members of a role have all of the privileges and permissions that are granted to the role.

You can add a role to multiple security roles, but you cannot create a circular membership where a particular role becomes a member of itself. A member of multiple security roles has the union of all the privileges and permissions that those roles grant.

Adding members to a security role is part of configuring security roles. This task is a step in the process for setting up Symantec Management Platform security.

See [“Creating and configuring security roles”](#) on page 65.

To add members to a security role

- 1 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 2 In the left pane, click **Account Management > Roles**.
- 3 On the **Roles** page, in the left pane, click the security role that you want to configure.
- 4 In the right pane, on the **Members** tab, click **Add Member** and then take one of the following actions:

To add a user account to the role Click **Add Account**.

To add another security role to the role Click **Add Role**.

- 5 In the **Select Account(s)** or **Select Role(s)** dialog box, select the user accounts or security roles that you want to add, and then click **OK**.
- 6 On the **Members** tab, verify that the list of members is correct. You can remove any that you do not want.
- 7 Click **Save changes**.

Assigning a Symantec Management Platform user account to a security role

You need to assign each Symantec Management Platform user account to the appropriate security roles. You need to be a member of the Symantec Administrators role, or a member of a role that has the Change Security privilege, to assign role membership. The account has the union of all the privileges and permissions that the roles to which it belongs grants.

See [“Creating and configuring Symantec Management Platform user accounts”](#) on page 191.

To assign a Symantec Management Platform account to a security role

- 1 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 2 In the left pane, click **Account Management > Accounts**.
- 3 On the **Accounts** page, in the left pane, click the account that you want to configure.

- 4 In the right pane, on the **Member Of** tab, make the appropriate settings.
- 5 Click **Add Role**.
- 6 In the **Select Role(s)** dialog box, select the security roles to which you want to add the account, and then click **OK**.
- 7 On the **Member Of** tab, verify that the list of security roles is correct. You can remove any that you do not want.
- 8 Click **Save changes**.

Adding security roles as members of other security roles

You can add a role as a member of other security roles. You need to be a member of the Symantec Administrators role or a member of a role that has the Change Security privilege to assign role membership. You can add a role to multiple security roles, but you cannot create a circular membership where a particular role becomes a member of itself. A role is granted the union of all the privileges and permissions that the roles to which it belongs provide.

Adding a role as a member of another role is the same as the other role adding the role to its membership. This method lets you add a particular role to a number of roles in a single procedure. The alternative would be to configure all of the other roles and specifically add the role to the membership of each.

Adding security roles as members of other security roles is part of configuring security roles. This task is a step in the process of setting up Symantec Management Platform security.

See [“Creating and configuring security roles”](#) on page 65.

To add a security role as a member of other security roles

- 1 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 2 In the left pane, click **Account Management > Roles**.
- 3 On the **Roles** page, in the left pane, click the security role that you want to configure.
- 4 In the right pane, on the **Member Of** tab, configure the appropriate settings.
- 5 Click **Add Role**.
- 6 In the **Select Role(s)** dialog box, select the security roles to which you want to add the role, and then click **OK**.
- 7 On the **Member Of** tab, verify that the list of security roles is correct. You can remove any that you do not want.
- 8 Click **Save changes**.

Assigning security permissions to folders and items

You can specify the non-inherited permissions that apply to each folder or item for each security role. These are combined with the permissions that are inherited from the parent folder. The combined permissions determine the access that the security role has to that particular folder or item. By default, any child folders or items inherit the combined set of permissions.

See [“Accessing the Security Role Manager”](#) on page 86.

This task is a step in the process for setting up Symantec Management Platform security.

See [“Setting up Symantec Management Platform security”](#) on page 62.

To assign security permissions to folders and items

- 1 In the Security Role Manager, in the **Role** drop-down list, select the security role for which you want to set permissions.
- 2 (Optional) In the **View** drop-down list, select an item category to view the folder structure that contains the relevant items.

If you want to view the full folder structure, select **All Items**.

- 3 In the left pane, select the folder or item for which you want to set permissions.

To preview the items of the selected folder in a separate pane, click the **List view** icon on the toolbar. In the middle pane, click the **Role view** icon to only view the items without the **Read** permission and click the **Deep view** icon to view the items as a flat list with ability to search within them.

Note that some items might be hidden by default. To see all items, click the **Show Hidden Items** icon on the toolbar. This functionality is only available for the roles that have the **Change Security** privilege assigned to them.

Warning: Use caution when editing the security permissions of a hidden item, because they are not designed to be modified.

- 4 In the right pane, in the **Item Permissions** panel, make the appropriate changes to the permission settings.
- 5 (Optional) If you want to configure permission inheritance for this folder or item, click **Advanced**.

See [“Customizing permission inheritance”](#) on page 79.

- 6 Click **Save changes**.

Customizing permission inheritance

By default, permission inheritance is enabled for all folders and items. Child folders and items inherit the security permissions for each role that is assigned to a folder. The inherited permissions cannot be modified on the child folders and items, but additional non-inherited permissions can be specified. The non-inherited permissions are applied directly to the folder or item and can be modified at any time. The permission settings on each folder or item are the combination of both the inherited and non-inherited settings. The combined set of permissions is then applied to any child folders or items. Any changes to permission settings for a folder are immediately applied to all of its child folders or items.

You can disable permission inheritance for any folder or item. This lets you remove some of the inherited permissions from the folder or item, but preserve them on its parent folder. The permission inheritance settings that you apply to a folder or item apply to every security role. You cannot customize inheritance settings for particular roles.

Warning: Disabling permissions inheritance on a folder or item can cause unexpected denials of access for user accounts. If you disable permissions inheritance, ensure that there are explicitly specified permissions on the folder or item for user accounts to have the appropriate access.

You can also remove all non-inherited permissions from folders or items, leaving only the inherited permissions. You may want to remove all non-inherited permissions to remove custom permissions that have been added to child folders or items. You may also use this feature to restore a standard set of permissions on all child folders and items.

See [“Assigning security permissions to folders and items”](#) on page 78.

This task is a step in the process for setting up Symantec Management Platform security.

See [“Setting up Symantec Management Platform security”](#) on page 62.

To customize permission inheritance for a folder or item

- 1 In the Security Role Manager, in the left pane, select the folder or item for which you want to configure permission inheritance.
- 2 In the right pane, click **Advanced**.
- 3 In the Permissions for: *Item Name* window, in the **Account/Group/Role** list, select the security role or user account for which you want to configure permissions.

If you want to add another security role or user account to the list, click **Add**. In the **Add Trustees** window, choose the appropriate security role or user account.

- 4 (Optional) In the **Permissions for** panel, change the permissions that are assigned to the selected security role for this folder or item.

You can use this feature only for the non-inherited permissions. You cannot edit the inherited permissions.

- 5 Take any of the following actions:

To inherit permissions from the parent folder

Check **Inherit the permission entries from parent object that apply to child objects.**

The inherited permission settings on the folder or item are updated to reflect the current permission settings on the parent folder.

To disable permissions inheritance

Uncheck **Inherit the permission entries from parent object that apply to child objects.**

You have the choice of copying the current inherited permissions from the parent folder, or removing all inherited permissions.

Any subsequent changes to the permission settings on the parent folder do not affect the permission settings on the folder or item.

To remove all non-inherited permissions from child folders and items

Check **Replace permissions on all child objects.**

The non-inherited permissions settings are cleared on all child folders and items, leaving only the inherited permissions.

- 6 Click **Save changes**.

- 7 (Optional) If you have disabled permission inheritance, in the **Inherited Permissions Behavior** dialog box, click the appropriate option:

Copy

The current inherited permissions are merged with the non-inherited permission settings on this folder or item.

Remove

The current inherited permissions are cleared, leaving only the non-inherited permissions.

Ensure that you have the appropriate non-inherited permissions on the folder or item before you select this option.

- 8 Click **Cancel** to close the Permissions for: *Item Name* window.

Predefined security roles

The Symantec Management Platform includes a set of predefined security roles that you can use. If the predefined security roles do not meet the needs of your organization, you can create

new ones. You can also edit the predefined security roles by specifying different privileges and permissions.

See [“Creating and configuring security roles”](#) on page 65.

Table 5-2 Predefined Symantec Management Platform security roles

Security role	Description
Everyone	<p>A top-level role that contains all roles and user accounts. The membership of this role is calculated automatically and cannot be modified manually.</p> <p>By default, this role has no privileges assigned. When you change permissions and privileges for this role, the changes are automatically applied to all other roles and user accounts.</p>
Symantec Administrators	<p>Has all security privileges and permissions assigned, so it has complete access to all aspects of the Symantec Management Platform and any installed solutions. You can modify the membership of this security role, but you cannot change its privileges and permissions.</p>
Symantec Supervisors	<p>Has the complete Management and most of the Right-click Menu privileges. Has limited System privileges assigned.</p> <p>Has the Read permission on resources, including security resources.</p> <p>Has the full access to Cloud-enabled Management settings, including setting up a new Internet gateway and generating the Symantec Management Agent installation package.</p>
Symantec Level 2 Workers	<p>Has the complete Management privileges and most of the Right-click Menu privileges assigned.</p> <p>Has the Read permission on resources, excluding security resources.</p> <p>Has the limited access to Cloud-enabled Management settings. For example, Symantec Level 2 Workers can create a Cloud-enabled Management Settings policy.</p>
Symantec Level 1 Workers	<p>Has no privileges assigned.</p> <p>Has the Read permission on resources, excluding security resources.</p>
Symantec Software Librarian	<p>Has the Software Management Framework privileges and the Right-click Menu Actions privileges assigned. The privileges are limited to those needed to create and manage software packages.</p>
Symantec Guests	<p>Has no privileges assigned.</p> <p>Has the Read permission on reports.</p>

Table 5-2 Predefined Symantec Management Platform security roles (*continued*)

Security role	Description
NT Authority\Authenticated Users	<p>Any user that logs in to Symantec Management Console, automatically becomes a member of this role. The membership of this role is calculated automatically and cannot be modified manually.</p> <p>By default, this role has no privileges or permissions assigned.</p>

Symantec Management Platform security management tasks

Table 5-3 Symantec Management Platform security management tasks

Task	Description
Configure password complexity and lockout settings.	<p>You can specify appropriate password complexity requirements to prevent Symantec Management Platform user accounts from creating weak passwords. Any changes that you make to the password complexity settings do not affect existing passwords. The password complexity rules are applied only when passwords are created or changed.</p> <p>See “Configuring password complexity and lockout settings” on page 83.</p>
Unlock locked out credentials.	<p>You can unlock internal the credentials that have become locked out after the maximum number of unsuccessful logon attempts has been exceeded.</p> <p>See “Unlocking locked out credentials” on page 85.</p>
Viewing and managing permissions of security roles.	<p>The Security Role Manager lets you view and set permissions for security roles. You can also use the Security Role Manager to take ownership of an item.</p> <p>See “Accessing the Security Role Manager” on page 86.</p>
Take ownership of a folder or item.	<p>You can take ownership of an item if its permissions are accidentally removed and the owner can no longer access it. After you take the ownership, you can reset the appropriate permissions and restore access for the original owner.</p> <p>See “Taking ownership of a folder or item” on page 87.</p>

Table 5-3 Symantec Management Platform security management tasks (*continued*)

Task	Description
Manage credentials.	Management solutions typically create credentials when they are needed to perform a task. See "Managing credentials" on page 88.

Configuring password complexity and lockout settings

The **Password Settings** page lets you configure the password complexity and lockout settings for internal credentials. These settings apply to internal credentials only: they do not apply to passwords that are managed externally, such as a Windows account. These complexity and lockout settings are often required to comply with an organization's access control policy.

You need to specify appropriate password complexity requirements to prevent Symantec Management Platform user accounts from creating weak passwords.

Note: Any changes that you make to the password complexity settings do not affect existing passwords. The password complexity rules are applied only when passwords are created or changed.

You cannot specify temporal restrictions such as allowing user accounts to log on only during certain time periods or on particular days of the week. To configure this type of restriction, you can use a scheduled task, a workflow, or an automation policy that disables and enables accounts at the appropriate times.

You cannot configure the maximum password age for internal credentials. The maximum password age for Windows credentials should be managed using a Windows policy.

See ["Unlocking locked out credentials"](#) on page 85.

You need to specify appropriate password lockout conditions to prevent unauthorized access to Symantec Management Platform. Any changes that you make to the password lockout settings are applied to all subsequent failed logon attempts. The maximum allowable unsuccessful attempts setting is not applied to the number of previous failed logon attempts.

To configure password complexity and lockout settings

- 1 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 2 In the left pane, click **Account Management > Password Settings**.

- 3 On the **Password Settings** page, on the **Password Complexity** tab, configure the password complexity settings:

Allow blank password Lets you specify whether a credential can have an empty password. If you enable this setting, the minimum password length is disabled.

By default, this setting is disabled.

Minimum password length Lets you specify the minimum number of characters that the password must contain. If you want to set the length to zero (0), you must also enable the **Allow blank password** setting.

The default value is six (6).

Minimum number of non-alphabetic characters Lets you specify the minimum number of non-alphabetic characters that the password must contain. Non-alphabetic characters are numbers (such as 1, 2, 3, etc.) and special characters (such as !, ?, &, etc.)

The default value is one (1).

Contain account name Lets you specify whether the password can contain the user account name. Note that this parameter is not case sensitive.

By default, this setting is disabled.

- 4 On the **Password Settings** page, on the **Password Lockout** tab, specify appropriate password lockout conditions:

Enable Credential Lockout	<p>Specifies whether to lock the credentials when the specified maximum number of unsuccessful logon attempts is reached.</p> <p>By default, this setting is enabled.</p>
Internal Credential Lockout Threshold	<p>Specifies the maximum number of logon attempts that a user may make with any particular credential. If a user attempts to authenticate with an incorrect password more than this number, the credential is locked for the specified lockout period.</p> <p>Unsuccessful logon attempts are counted from when the credential is created. The failed attempts do not need to happen within a minimum time period. There is no maximum time after which a failed attempt is no longer counted.</p> <p>If you change this setting to reduce the maximum number of unsuccessful attempts allowed, the new value is not applied to any account until the next logon attempt. If the next attempt is successful, the count is reset to zero (all previous failures are erased). However, if the next attempt fails, the count of failed attempts is evaluated. If the maximum number is reached (or possibly already exceeded), the account is locked.</p>
Lockout Duration	<p>Specifies the duration that a locked out credential cannot be used. The default period is 1800 minutes (30 hours).</p> <p>All logon attempts that the user makes during this time period fail, even if the correct credentials are supplied. When the lockout period expires, the same credentials are valid again. No automatic password reset is required.</p> <p>You can specify an infinite lockout period by entering a value of -1. In this scenario, a locked credential remains locked until an administrator manually unlocks the credential.</p> <p>See “Unlocking locked out credentials” on page 85.</p>

- 5 Click **Save changes**.

See [“Symantec Management Platform security management tasks”](#) on page 82.

Unlocking locked out credentials

The **Unlock Credentials** page lets you unlock internal credentials that have become locked out after the maximum number of unsuccessful logon attempts has been exceeded.

See [“Configuring password complexity and lockout settings”](#) on page 83.

To unlock locked out credentials

- 1 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 2 In the left pane, click **Account Management > Unlock Credentials**.
- 3 On the **Unlock Credentials** page, in the list of locked credentials, select the credential that you want to unlock.
- 4 Click **Unlock Credentials**.

Accessing the Security Role Manager

The Security Role Manager is a special console that lets you view and set permissions for security roles. The console lets you select a particular security role and view the permissions that are associated with each item for that security role. You can view the items by type, or view all the available items, and select the folder or item on which to set permissions. By default, child items and folders inherit all permissions on a folder. You can modify permission inheritance to suit your requirements.

You can also use the Security Role Manager to take ownership of an item. You may need to take ownership if permissions on an item are removed accidentally so that the owner no longer has access to it. By taking ownership of an item, you can reset the appropriate permissions and restore access for the original owner.

Table 5-4 Ways to access the Security Role Manager

Option	Description
Directly from the Symantec Management Console Settings menu.	The Security Role Manager opens with your security role selected, and the All Data Classes view shown.
From the right pane of the Roles page.	The Security Role Manager opens with the appropriate security role selected, and the All Data Classes view shown.
From the Actions menu for a security role.	The Security Role Manager opens with the appropriate security role selected, and the All Data Classes view shown.
From the right-click menu for an item or folder in the left pane.	You would normally use this method to set permissions on a particular item or folder. The Security Role Manager opens with your security role selected, and the appropriate folder selected.

To access the Security Role Manager from the Symantec Management Console menu

- ◆ In the Symantec Management Console, on the **Settings** menu, click **Security > Permissions**.

To access the Security Role Manager for a specific security role

- 1 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 2 In the left pane, click **Account Management > Roles**.
- 3 On the **Roles** page, in the left pane, click the security role that you want to configure.
- 4 Do one of the following:
 - In the right pane, click **Show Security Role Manager Console**.
 - Click **Actions > Security Role Manager**.
 - Right-click the security role that you want to configure and then click **Security Role Manager**.

To access the Security Role Manager for a specific folder

- 1 In the Symantec Management Console, open a view that contains the folder on which you want to set security permissions.
- 2 In the left pane, right-click the folder and then click **Security**.

Taking ownership of a folder or item

You can also use the Security Role Manager to take ownership of an item. This may be required if permissions on an item are removed accidentally so that the owner no longer has access to it. By taking ownership, you can reset the appropriate permissions and restore access for the original owner.

To take ownership of a folder or item, you require the Take Ownership privilege and the Full Control permission on the folder or item. The Symantec Administrator role has this privilege, and has this permission on all items and folders.

See [“Customizing permission inheritance”](#) on page 79.

To take ownership of a folder or item

- 1 In the Security Role Manager, in the left pane, select the folder or item for which you want to take ownership.
- 2 In the right pane, click **Advanced**.
- 3 In the Permissions for: *Item Name* window, click **Take Ownership**.
- 4 Click **Save changes**.
- 5 Click **Cancel** to close the Permissions for: *Item Name* window.

Managing credentials

Credential manager provides a secure storage location for user names and passwords. Your installed management solutions define the types of credentials that the credential manager stores.

See [“Security permission categories”](#) on page 420.

See [“Credential Manager permissions”](#) on page 437.

Access to credentials is controlled with the built-in role-based security of the Symantec Management Platform.

Management solutions typically create credentials when they are needed to perform a task. To define a credential manually, you need to know the credential type that is used and the information that is required for that credential type.

When a credential is created, only the creator is granted access. Editing a credential lets you update the password and lets you grant access to additional users and groups.

You can also delete the credential. Before you delete a credential, make sure that it is not required as part of an active management task.

To create a credential

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, click **Monitoring and Alerting > Credential Settings > Credentials Management**.
- 3 In the right pane, click **Add Credentials**.
- 4 In the **Add Credential** dialog box, select a credential type and then provide the required values.
- 5 Click **OK**.

To edit a credential

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, click **Monitoring and Alerting > Credential Settings > Credentials Management**.
- 3 In the right pane, select a credential and then click **Edit**.
- 4 In the **Edit Credential** dialog box, update the credential, and then click **OK**.

Configuring schedules

This chapter includes the following topics:

- [How Symantec Management Platform uses schedules](#)
- [Components of a Symantec Management Platform schedule](#)
- [Managing shared schedules](#)
- [Configuring a schedule](#)
- [Viewing the Notification Server internal schedule calendar](#)

How Symantec Management Platform uses schedules

Symantec Management Platform uses schedules for tasks and policies.

See [“Components of a Symantec Management Platform schedule”](#) on page 91.

Table 6-1 Schedule uses

Use	Description
Scheduling server tasks and server policies	<p>Many Symantec Management Platform operations are scheduled to occur at regular intervals. Some of these operations need to be performed frequently. For example, updating the membership of resource groups and filters, or they may be less frequent, such as purging old records from the CMDB.</p> <p>These schedules are usually configured to repeat at regular intervals, and they remain active for an indefinite period.</p>

Table 6-1 Schedule uses (*continued*)

Use	Description
Scheduling agent tasks	<p>Schedules may be used when you want to perform operations on managed computers. For example, rolling out a patch to fix a vulnerability in an application or gathering inventory for compliance purposes. You would usually want to perform the operation as soon as possible, and you would want to perform it one time only.</p> <p>You can schedule agent tasks to run:</p> <ul style="list-style-type: none"> ■ Immediately ■ Immediately, if a maintenance window is open ■ The next time a user logs on to the computer ■ The next time the computer is started. <p>On some occasions you may want to schedule the operation to take place at a specific date and time. For example, 9:00 P.M. next Sunday evening, to ensure that it does not interfere with the user's ability to work.</p> <p>On rare occasions you may need to schedule a task to repeat. However, a repeating operation would usually be considered a task-based policy.</p>
Scheduling agent policies	<p>An agent policy is a statement about how a computer should be managed.</p> <p>For example, an agent policy may do the following:</p> <ul style="list-style-type: none"> ■ Disallow software from being run ■ Require software to be installed ■ Require that inventory information about a computer be no older than N days <p>To function correctly, some agent policies need to be scheduled to run at appropriate intervals. For example, a software compliance policy needs to periodically check that the computer is in compliance, and perform the appropriate remediation if it is not. Likewise, an inventory policy needs to ensure that the inventory data is current.</p> <p>These schedules are usually recurring schedules with a possible repetition during the working day. Agent policies are often scheduled to run when the computer starts up, or when a user logs on. When you set up these schedules, you also need to consider how they interact with the maintenance windows that are configured on the managed computers.</p> <p>See “Configuring the global agent settings” on page 236.</p> <p>See “Configuring the targeted agent settings” on page 237.</p>
Scheduling agent maintenance windows	<p>A maintenance window schedule is essentially a recurring schedule that has a duration. You do not need to schedule maintenance windows using computer startup, user logon, or other events. Maintenance windows have no need for any repetition during the working day.</p> <p>See “Configuring maintenance window policies” on page 244.</p>

Components of a Symantec Management Platform schedule

Symantec Management Platform schedules let you perform both once-off and repeating operations on the Notification Server computer and the managed computers at appropriate times, without requiring manual intervention. For example, resource filters need to be updated frequently, the CMDB needs to be purged regularly, and packages must be refreshed at appropriate intervals. All of these tasks should be scheduled to run at whatever times and frequencies best suit the needs of your organization.

See [“How Symantec Management Platform uses schedules”](#) on page 89.

Symantec Management Platform uses two types of schedules:

- Shared These are defined on Notification Server as shared items that are available for any scheduled operation to use.

See [“Managing shared schedules”](#) on page 93.
- Custom These are configured independently within each task, policy, or rule that is scheduled. They cannot be shared with any other tasks, policies, or rules.

Table 6-2 Components of a schedule

Component	Description
Active period and time zone	<p>The active period and time zone define the time period within which a schedule may occur.</p> <p>All schedules, triggers, and modifiers have the following properties:</p> <ul style="list-style-type: none"> ■ Time Zone The time zone in which the task is scheduled to run. The time zone may be Local, Server, or UTC. ■ Start Date The date and time when the schedule's active period begins. A schedule cannot be triggered before its start date. ■ End Date The date and time when the schedule's active period ends. If the end date is not specified, the schedule remains active indefinitely. A schedule cannot be triggered after its end date. <p>A schedule cannot run outside its active period. This applies even if the schedule was triggered within its active period, but was prevented from running at that time by a modifier.</p>

Table 6-2 Components of a schedule (*continued*)

Component	Description
Triggers	<p>A trigger is an event that causes the schedule to become active. A trigger may be a specific time and date, or an event such as a user logging on to a computer. Triggers control when the schedule occurs and repeats. If a schedule contains multiple triggers, it runs each time that any one of its triggers occurs.</p> <p>Schedule triggers may have the following properties:</p> <ul style="list-style-type: none"> ■ Exact Determines the behavior when a scheduled task cannot be performed at the exact time at which it is scheduled. If the property is set to true, the scheduled task runs at the exact time, or not at all. If the conditions are such that the task cannot be performed at the exact scheduled time, the scheduled task is not performed. If the property is set to false, the scheduled task runs at the exact time, or as soon as possible after the scheduled time. For example, a task is scheduled to run every night at 2:00 A.M., but the computer is always off at that time. The Exact setting lets you run the task whenever the computer is turned on after that time. This property applies to logon, startup, and other events, as well as specified times. ■ Duration The length of time that the schedule is active. The duration may be up to 24 hours. ■ Repetition The interval at which the task should be repeated during the schedule's active period. The repetition interval may be up to 24 hours.
Modifiers	<p>Modifiers are the additional conditions that are required for the schedule to be triggered. All of the modifiers apply to all of the triggers.</p> <ul style="list-style-type: none"> ■ Only when a user is logged on When the trigger occurs on a target computer, the Symantec Management Agent on that computer checks to ensure that a user is logged on before it runs the schedule. If no user is logged on, the schedule is not run on that computer. ■ Only when no user is logged on When the trigger occurs, the target computer is checked to ensure that no user is logged on. If a user is logged on, the schedule is not run on that computer.

Managing shared schedules

Any number of scheduled items (such as policies, tasks, or replication rules) may use a shared schedule. The alternative to using a shared schedule is to define a custom schedule within the policy or task.

See [“Components of a Symantec Management Platform schedule”](#) on page 91.

Shared schedules cannot override maintenance windows. If you want a scheduled item to run outside a maintenance window, you need to configure the appropriate custom schedule.

A set of default shared schedules is supplied with Symantec Management Platform. You can modify these to suit your requirements, but you cannot delete them. For example, you can configure the business hours schedule to run at regular intervals during your normal working hours. You may configure the package refresh schedule to run at a suitable time outside working hours. You can also create any new shared schedules that you require and delete them when they are no longer required.

You can enable or disable each shared schedule as appropriate. All enabled shared schedules are available to any scheduled item. If you disable a shared schedule, any scheduled item that uses the schedule is disabled.

See [“Viewing the Notification Server internal schedule calendar”](#) on page 95.

To manage shared schedules

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Shared Schedules**.
- 2 On the **Shared Schedules** page, do any of the following:

To add a new schedule	Click Add Schedule and then, in the Schedule Editor, specify the appropriate details. See “Configuring a schedule” on page 94.
To edit a schedule	Click the schedule name and then, in the Schedule Editor, specify the appropriate details. See “Configuring a schedule” on page 94.
To enable a schedule	Check the appropriate check box. If you want to disable the schedule, clear the check box.
To delete a schedule	At the right end of the appropriate row, click Delete .
To see how many resources currently use a schedule	Check the Resources check box. The amount of the resources that currently use a schedule is added to the Used By column.
To see which items currently use a schedule	In the Items Currently Using drop-down list, select the appropriate schedule. The names of all the items (such as tasks, policies, and replication rules) that use the selected schedule are shown in the lower panel. If you have checked the Resources check box, then also the names of the resources are displayed.

Configuring a schedule

The **Schedule Editor** lets you configure a schedule to suit your requirements.

See [“Components of a Symantec Management Platform schedule”](#) on page 91.

See [“Managing shared schedules”](#) on page 93.

To configure a schedule

- 1 In the **Schedule Editor** window, in the **Name** box, type the schedule name.
- 2 Under **Schedule Task**, select the schedule frequency or trigger.
- 3 In the **Details** tab, specify the schedule start time, and the days, weeks, or months on which to run.

- 4 If you want the schedule to be active for a particular range of dates, in the **Advanced** tab, specify the appropriate start and end dates.

By default a new schedule is active as soon as it is created (from the current date). The schedule remains active indefinitely (no end date is specified).
- 5 If you want the schedule to repeat a task at regular intervals each time the schedule runs, in the **Advanced** tab, check **Repeat Task**.

Specify the appropriate frequency and duration.
- 6 If you want this schedule to contain multiple schedules, check **Use Multiple Schedules**.
- 7 For each additional schedule that you want to add to this schedule, click **New**, and then complete steps 2 to 5.
- 8 Click **OK**.

Viewing the Notification Server internal schedule calendar

You can view Notification Server schedule information in the Notification Server internal schedule calendar. The scheduled items that you can view in the Calendar include tasks running on Notification Server, policies, and automation policies. They also include shared schedules, blackout periods, maintenance windows, and Notification Server internal schedules. Symantec solutions may add additional scheduled items to the calendar.

See [“Components of a Symantec Management Platform schedule”](#) on page 91.

The following types of scheduled items are displayed:

Period items	These define only a start time, and run for an indefinite period. Examples include maintenance windows, blackout periods, and shared schedules.
Event items	These have a defined end time. Examples include tasks, jobs, custom schedules, and policies. Note that policies are not always run at the times that are shown in the calendar. Policies are not as deterministic as tasks, so may be subject to delay. Tasks and jobs are always run at the times that are shown in the calendar.

The Calendar view lets you see what schedules are configured for particular time periods, such as specific days, weeks, or months. In both the Week view and the Month view, you can click a particular day to open the Day view for that day.

Some scheduled items use shared schedules, rather than define their own schedules. Shared schedule relationships are represented in the left pane of the Day view. The scheduled items are grouped under the shared schedule to which they refer.

Each schedule has an associated symbol that links it to the appropriate configuration page, if one is available. You can click the symbol to drill down to the configuration page, which opens in a new window. If no configuration page is available for a schedule, the default calendar symbol is used and no drill-down functionality exists.

See [“Managing shared schedules”](#) on page 93.

See [“Configuring a schedule”](#) on page 94.

To view the Notification Server schedule calendar

- 1 In the Symantec Management Console, in the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Settings > Notification Server** and then click **Internal Schedules Calendar**.
- 3 On the **Calendar View for Internal NS Schedules** page, in the **View** drop-down list, select the view that you want to use.
- 4 Select the time period that you want to view by clicking the appropriate symbol:

Day	Shows the details of each schedule that runs one or more times per day. The schedules are listed in order of their start times. The left pane lists the schedules, and the right pane shows their occurrences in the calendar. Day view is the default view.
-----	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Each occurrence of a period item is displayed as a diamond. Each occurrence of an event item is normally displayed as a bar, but those that occur with very short intervals are displayed as small diamonds. For clarity on screen, events with an interval less than 15 minutes (by default) are omitted.

The background color identifies the business hours that are defined for the organization.

Week	Shows the details of each schedule that runs less than one time per day but at least one time per week.
------	---------------------------------------------------------------------------------------------------------

Month	Shows the details of each schedule that runs less than one time per week are displayed. Period items are omitted and event items are summarized to their start times, end times, and titles.
-------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- 5 To view earlier or later time periods, click **Previous** or **Next**, whichever is appropriate.

Configuring sites and site servers

This chapter includes the following topics:

- [About site services](#)
- [About site maintenance](#)
- [Managing sites](#)
- [Managing subnets](#)
- [Managing site servers](#)
- [About configuring the site service settings](#)

About site services

The Symantec Management Platform can host several types of middleware components, such as package service, task service, monitor service, and network boot service. Middleware components can be installed on computers other than the Notification Server computer. These services act as the first point of contact for the Symantec Management Agents, thus reducing the load on Notification Server.

The official name for a middleware component is “site service.” Any computer that hosts a site service is known as a site server. A site server can have one or more site services installed on it. For example, if you install the package server site service (the “package service”) onto a computer, that computer becomes a site server.

Site servers can assist Notification Server. Site servers can extend the architecture, improve distribution efficiency, and reduce network bandwidth requirements.

Notification Server handles the deployment, configuration, and ongoing maintenance of site services.

Notification Server performs the following functions for site management:

- Handles the deployment and removal of site services to and from site servers
- Ensures that the site service is installed only on the computers that satisfy the minimum system requirements

You use site maintenance to create logical groups of endpoints to balance the load on site servers. For example, you can distribute packages efficiently to your Symantec Management Agents with multiple package servers. The package servers handle most of the package distribution functions, which frees up Notification Server to perform other activities.

See [“About site maintenance”](#) on page 98.

About site maintenance

Site maintenance is the management of sites, subnets, and site services in your organization. You can manage your computers according to site and subnet, which lets you control groups of computers while you minimize bandwidth consumption. A site is typically a physical location in your organization (such as a particular building, or a level of a building). A subnet is a range of logical addresses on your network.

Under normal operating conditions, each package server or task server services only the Symantec Management Agents that exist within the assigned sites. If no sites have been defined, all site servers are available to service all Symantec Management Agents (although this method is not recommended).

If no sites are defined for a package server or a task server, Notification Server uses the following rules:

- Notification Server first tries to find any site servers on the same subnet as the requesting computer. If any are found, these site servers are returned to the Symantec Management Agent.
- If no site servers are in the same subnet as the requesting computer, all site servers are returned to the Symantec Management Agent.

You can assign site servers to sites by using the following methods:

- Assign the subnet that contains the site server to a site.
See [“Managing subnets”](#) on page 103.
- Assign the site server to a site.
See [“Assigning a site server to a site manually”](#) on page 108.
- Use Active Directory import to perform the task.

Active Directory import overrides any subnets and sites that conflict with it. For example, if you manually assign subnets to a site that conflicts with the data from Active Directory import, the Active Directory information is used.

After the list of available site servers is returned to the Symantec Management Agent, the agent chooses the most suitable site server.

Site servers and managed computers may have multiple NICs and IP addresses; therefore, they may belong to more than one site through subnet assignment.

See [“About site services”](#) on page 97.

See [“Managing sites”](#) on page 99.

See [“Managing site servers”](#) on page 106.

See [“Managing subnets”](#) on page 103.

Managing sites

You need to set up all the sites that you require in your organization. You can run a site import rule to automatically collect the site information for your organization from Active Directory. You can also create sites manually and assign the appropriate subnets and site servers to them.

The types of site can be as follows:

- Intranet sites - for internal clients
- Internet sites - for cloud-enabled agents

See [“Configuring sites and site servers to serve cloud-enabled agents”](#) on page 265.

To manage sites

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 Do any of the following:
 - Create a new site.
 - 1 In the left pane, click **New > Site**.
 - 2 In the **New Site** window, in the **Name** box, type the new site name.
 - 3 If you want to assign subnets to the site immediately, specify the appropriate subnets.
 - 4 Click **OK**.

- Modify a site.
- 1 In the left pane, select the site that you want to modify, and then click **Configure**.
 - 2 To change the site name, in the **Edit Site** window, in the **Name** box, type the new name.
 - 3 To change the subnets that are assigned to the site, specify the appropriate subnets.
 - 4 Click **OK**.
- Delete a site.
- ◆ In the left pane, select the site that you want to delete, and then click **Del**.
- Any subnets that are assigned to the site are not deleted. They become unassigned and may be assigned to a different site. Any site servers inside the affected subnets are not used until they are assigned to a different site.
- Remove a manually assigned site server from a site.
- ◆ In the left pane, under the site server, select the site that you want to remove, and then click **Del**.
- The site server is not affected, and it continues to serve any other sites to which it is assigned. This option applies only to the site servers that are manually assigned to sites. A site server that belongs to a site through its subnet membership cannot be removed from that site.
- Remove a subnet from a site.
- ◆ In the left pane, under the site, select the subnet that you want to delete, and then click **Del**.
- Deleting a subnet makes the subnet unassigned to any site. Any encompassed subnets that are not manually assigned to a site also become unassigned. Any site servers on the subnet, or the encompassed subnets, no longer serve the site. However, they continue to serve any sites to which they are manually assigned.
- Manage manually assigned agents.
- You can assign agents to a site and remove any that you no longer require.
- See [“Managing manually assigned agents”](#) on page 101.
- Create targeted site settings policy.
- Targeted site settings policy lets you configure and apply settings to a specific site. For example, you can limit the number of simultaneous outbound data transfers from a site.
- See [“Configuring site settings”](#) on page 101.

Managing manually assigned agents

A manually assigned agent is a computer that has been manually assigned to a site or site server rather than assigned through its subnet. You may want to manually assign particular computers to a site or site server to break away from the subnet assignment. You can manually assign new agents to a site by assigning the relevant resource targets to it. You can remove any agents that you don't want in the site by assigning the appropriate resource targets to a different site.

Note: When the manually assigned agent is a Task Server, the change does not formalize unless you reset the Symantec Management Agent on the computer. One way to reset the Symantec Management Agent is to click **Reset Agent** on the **Task Status** tab in the Symantec Management Agent. Another way is to run the Reset Task Agent task on the computer.

To manage manually assigned agents

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the left pane, expand the site or site server that you want to modify, and then click **Manually Assigned Agents**.
- 3 On the **Manually Assigned Agents** page, do any of the following:

Add manually assigned agents to a site or site server.	Click New and then, in the Select a group window, select or create the appropriate resource targets.
Reassign manually assigned agents to another site.	Note that this option is available only under the Site node, not the Site Services node. Select the appropriate resource targets, and then click Assign to Site . In the Select a site window, select the appropriate site, and then click OK .
Remove manually assigned agents from a site or site server.	Select the appropriate resource targets, and then click Delete .

Configuring site settings

The targeted site settings policy lets you configure and apply download settings to the sites.

This feature is available starting from IT Management Suite version 8.5 RU2.

Configuring the targeted site settings policy for each site is not required. If you do not configure the policy for a site, its outbound data transfer settings remain unlimited and the agents can download packages from any source.

Note: If the default site settings policy is applied to a site and you create another site settings policy and apply it to the same site, the computers in this site do not receive the second policy and continue to work according to the policy that was applied first.

See [“Managing sites”](#) on page 99.

To configure site settings

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the left pane, expand **Site Server Settings**, and do one of the following:
 - To create a custom site settings policy, right-click **Targeted Site Settings**, and then click **New > Site Settings Policy**.
 - To configure and enable the predefined **Internet Site Settings** or **Non-Internet Site Settings** policies, expand **Targeted Site Settings**, and then click the policy that you need.

- 3 On the site settings policy page, configure the following options:

Outbound Connection Settings

The **Number of simultaneous data transfers** option lets you limit the number of outbound data transfers from a site to which the Symantec Management Agent belongs. This limitation lets you ensure that the download of many packages is completed even when the site has limited bandwidth.

For example, at a site with 1000 devices, only 10 devices can download a package from outside of a site simultaneously.

Note: In a hierarchy, you can configure this option only on parent Notification Server. After you replicate the site settings policy to child Notification Server, this option cannot be edited.

(Windows only) The **Maximum overall transfer speed** option lets you specify the maximum data transfer rate for the whole site. The agents of this site can use the specified speed for downloading packages from a source that is located outside of the site. The maximum data transfer rate for each downloading agent is calculated based on the specified **Maximum overall transfer speed** and the number of downloading agents.

Prevent Downloads

The **Prevent Downloads** options let you limit the sources from which the agents are allowed to download packages. For example, you can prevent package downloads directly from Notification Server.

These options are available starting from IT Management Suite version 8.5 RU3.

Applied to

Specify a target for the site settings policy.

Warning: The target of this policy must contain only **Site** resources. The policy does not work if its target contains **Computer** or **User** resources.

- 4 Turn on the policy.

At the upper right of the page, click the colored circle, and then click **On**.

- 5 Click **Save changes**.

Managing subnets

You need to create all the subnets in your organization and assign them to the appropriate sites. You can resynchronize subnets when necessary and delete any subnets that no longer exist. Note that the **Package Refresh** shared schedule that runs daily by default, performs the resynchronization automatically.

Subnets can be determined from the basic inventory data that is imported from Active Directory or added manually. You can run a subnet import rule to automatically collect the subnet information from Active Directory.

Subnets are always suffixed with the number of bits that are set in the network mask, for example 192.168.0.0/24. The subnets are always displayed in a hierarchical tree. Resource scoping applies, so you can see only the subnets that contain resources to which you have access.

You need to assign each subnet to the appropriate site. By default, any encompassed subnets (a subnet whose IP range is wholly contained within another subnet) are automatically assigned to the same site. However, you can manually override subnet encompassment by explicitly assigning an encompassed subnet to a different site. By default, encompassed subnets are displayed under their parent subnets in the left pane. However, when an encompassed subnet is manually assigned to a different site from its parent, it is displayed under the site to which it is assigned.

Any site servers on a subnet are automatically assigned to the same site as the subnet. This assignment is not broken if you manually assign a site server to a different site. A site server can be manually assigned to any number of sites, in addition to the site that it serves through its subnet assignment.

To manage subnets

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 Do any of the following:

- Create a new subnet
- 1 In the left pane, click **New > Subnet**.
 - 2 In the **New Subnet** dialog box, specify the subnet network address, subnet mask, the site to which you want to assign this subnet, and then click **OK**.
- When you press **Tab** or click in this box after typing the subnet network address, a mask is automatically selected according to the following rules:
- The system examines the first octet of an IPv4 address to determine if it is a class A, B, or C subnet. It then selects the appropriate default mask.
 - If the network address is more specific (i.e. more non-zero octet) than allowed for that class, then additional bytes are set in the default mask.
 - If the address is not in a recognized format, or the last octet is non-zero, then no default mask is suggested.
- You can edit the default mask manually if necessary. Note that after you manually edit the subnet mask, updating the network address in the **Subnet** box no longer updates the mask.
- Delete a subnet
- In the left pane, expand **Site Management > Subnets**, select the subnet that you want to delete, and then click **Del**.
- If you delete a subnet that you created manually, it is deleted permanently. However, any subnets that were imported from basic inventory or from Active Directory are restored when the data is refreshed.
- Assign a subnet to a site
- 1 In the left pane, expand **Site Management**, and then click **Subnets**.
 - 2 In the right pane, select the appropriate subnet, and then click **Assign to site**.
 - 3 In the **Select a site** dialog box, select the site to which you want to assign the subnet, and then click **OK**.
- Resynchronize subnets
- 1 In the left pane, expand **Site Management**, and then click **Subnets**.
 - 2 In the right pane, click **Re-synchronize Subnets**.
- Notification Server refers to the CMDB for the current subnet information. It reads the subnet assignment that is included in the results of the latest Agent Inventory scan. Notification Server then updates the list of subnets accordingly.

Managing site servers

You need to create all the site servers that you require in your organization and assign them to the appropriate sites. To create site servers, select the computers that you want to use and specify the site services that you want to install on each.

Note: When you add a Package Server to the environment, the package service might be interrupted for some time. The interruption occurs because it takes some time until the packages replicate from Notification Server to the Package Servers. The Package Servers can start serving the agents only after the replication.

You can also modify existing site servers by adding or removing site services. Notification Server then deploys the appropriate installation packages to the selected computers, and removes any that are no longer required. Note that the changes are made when the Symantec Management Agents on the target computers make their next configuration request, so it may not happen immediately.

To ensure that the site services are properly installed and configured, Symantec recommends that you install the site services through the Symantec Management Console.

Note: The package server computer must have IIS 7.0 or IIS 8.5 installed to work with Deployment Solution.

For more information on how Deployment Solution uses site servers, see the *Deployment Solution User Guide*.

When a site server is selected, the **Site Services** page shows statistics for each site service that is installed on it. The collapsed view shows summary details, while the expanded view opens a pane for each site service that shows full details and graphical information. Each site service pane also includes a link to the corresponding global settings configuration page.

The title bar for each site service contains a symbol that shows its current status:

Green	The service is installed and running on the site server.
Yellow	The service is not installed. The service is installed but currently disabled or in warning state on the site server.
Red	The service has an error. For example, one or more packages are invalid on the package server.

To manage site servers

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.

- 2 Do any of the following:

Create a site server.

- 1 In the left pane, click **New > Site Server**.
- 2 In the **Select Computers** window, select the computers to which you want to add site services and click **OK**.

The list in the left panel contains all the computers that are available to be used as site servers. When you install the Symantec Management Platform, you need to allow a few minutes for the system to populate this list.

- 3 In the **Add/Remove Services** dialog box, check the appropriate check boxes to select the site services that you want to install on each site server and click **Next**.

All of the available site services are listed under each computer, letting you select any combination of services for each computer. The check boxes for any service types that are not allowed to be installed on a particular computer are grayed out. Right-click the grayed out check box and click **View Prerequisites for the Site Service** to view the list of prerequisites for installing the specific site service.

You can group the list by site servers or by services. Selecting a parent node on the list selects all of its children.

If any check box is already checked, that indicates the corresponding site service is already installed. If you want to remove it, uncheck the check box.

- 4 Click **OK**.

Modify a site server.

- 1 In the **Detailed Information** table, ensure that the site servers view is selected, and then select the appropriate site server.
- 2 Click the **Edit** symbol.

Manually assign a site server to a site.

Select the appropriate site server, and then click **Assign to Site**.

See [“Assigning a site server to a site manually”](#) on page 108.

See [“Managing manually assigned agents”](#) on page 101.

Remove a manually assigned site server from a site.

In the left pane, under the site server, select the site that you want to remove, and then click **Del**.

The site server is not affected, and it continues to serve any other sites to which it is assigned. This option applies only to the site servers that are manually assigned to sites. A site server that belongs to a site through its subnet membership cannot be removed from that site.

Configure global site server settings.

- 1 In the left pane, expand **Site Management > Settings**, and then click **Global Site Server Settings**.
- 2 On the **Global Site Server Settings** page, configure the settings, and then click **Save changes**.

See [“Configuring global site server settings”](#) on page 109.

Note that you can configure site server settings for each site server separately.

See [“Configuring individual connection settings for a site server”](#) on page 110.

Configure site server communication profile.

- 1 In the left pane, expand **Site Management > Site Servers**, expand the site server for which you want to configure the communication profile, and then click **Communication Profile**.
- 2 In the right pane, click the name of the communication profile.
- 3 In the communication profile dialog box, make the necessary changes, and then click **Save changes**.

See [“Configuring a site server communication profile”](#) on page 112.

Assigning a site server to a site manually

Site servers automatically serve the site to which their parent subnet is assigned. Site servers may have multiple NICs/IPs and be in more than one subnet, so may therefore belong to more than one site. You can also manually assign each site server to one or more other sites. The **Manually Assigned** column in the **Detailed Information** table indicates whether the site server is manually assigned to the site.

See [“Managing site servers”](#) on page 106.

See [“Configuring sites and site servers to serve cloud-enabled agents”](#) on page 265.

When you manually assign a site server to a site, only the site server is assigned to the selected site. The subnet to which the site server belongs is not affected.

To assign a site server to a site manually

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the **Detailed Information** table, ensure that the site server view is selected, and then select the appropriate site servers.
- 3 Click **Assign to Site**.
- 4 In the **Select a Site** window, select the site to which you want to assign the site server.
- 5 Click **OK**.

Configuring global site server settings

The **Global Site Server Settings** page lets you configure the security settings and distribute intranet certificates or Cloud-enabled Management (CEM) certificates.

Note that you can also configure the settings for each site server separately.

See [“Configuring individual connection settings for a site server”](#) on page 110.

This task is a step in the process for preparing your environment for Cloud-enabled Management.

See [“Preparing your environment for Cloud-enabled Management”](#) on page 254.

To configure global site server settings

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the left pane, expand **Site Management > Site Servers**, and then click **Global Site Server Settings**.
- 3 On the **Global Site Server Settings** page, configure the following settings:

Security Settings

Lets you create the Agent Connectivity Credential (ACC) on the site servers, provided the ACC is not a domain account. During this procedure, you can re-enable the created local account if it has been locked out and create the ACC even if the site server is also a domain controller.

Persistent Connection

Lets you enable the **Persistent Connection** for site server.
Note that you must also configure and enable the persistent connection in the site server communication profile(s).

See [“Enabling persistent connection in your environment”](#) on page 148.

See [“Configuring a site server communication profile”](#) on page 112.

Web Configuration

The **Configure HTTP on site servers** section lets you specify the HTTP port that is used on the site servers.

The **Configure HTTPS on site servers** section lets you configure the HTTPS port and intranet certificate for site servers. The intranet certificate is delivered to all site servers.

The **Configure CEM web on site servers** section lets you configure the port for CEM connections and CEM certificate. The CEM certificate is delivered to the site servers that are assigned to the Internet sites. The CEM certificate is required on the site servers that serve the cloud-enabled client computers.

Note that for HTTPS and CEM bindings, the port configuration is separated from the certificate rollout. You can change the ports without the need to reinstall the certificates.

Specify the following settings for one or both of the bindings:

- **Port** - port at the web server where HTTPS or CEM binding is created.
- **Force overwrite binding settings** - controls if the binding on specified port is recreated if it already exists.
- **Install certificate** - controls if the certificate is installed.
- **Master certificate** - for the intranet certificate, you can select the master certificate that is used to sign the certificate that is installed at the web server.

After you configure the port for HTTPS or CEM binding, site server creates corresponding binding, and starts performing its activities on this port. Also, the persistent connection starts working on this port.

Warning: If you uncheck the **Configure HTTPS binding** option, the WebSocket server does not start on the site server and the persistent connection will not be available.

- 4 Click **Save changes**.

Configuring individual connection settings for a site server

By default, the **Global Site Server Settings** policy configures the connection settings and distributes the intranet certificate or the CEM certificate globally to the site servers.

However, you can also configure the connection settings for each site server separately. The individual settings override the global settings.

See [“Configuring global site server settings”](#) on page 109.

To configure individual connection settings for a site server

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the left pane, expand **Site Management > Site Servers**, and then click the site server for which you want to configure individual settings.
- 3 In the right pane, configure the following settings:

Web Configuration

To configure individual settings:

- 1 Click **Override the global settings by custom settings**.
- 2 In the custom settings dialog box, edit the necessary settings.
- 3 Enable the settings.

 At the upper right of the page, click the colored circle, and then click **On**.

 Note that only after you enable the individual settings, the global settings are overwritten.
- 4 Click **Save changes**.

Persistent Connection

To configure individual settings:

- 1 Click **Override the global settings by custom settings**.
- 2 In the custom settings dialog box, check the **Enable Persistent Connection** option if you want to enable persistent connection for this site server.
- 3 Enable the settings.

 At the upper right of the page, click the colored circle, and then click **On**.

 Note that only after you enable the individual settings, the global settings are overwritten.
- 4 Click **Save changes**.

Communication Profile

Lets you view and edit the communication profile that is applied to this site server.

Note that if you edit the communication profile, the changes also affect all other computers to which this communication profile applies.

See [“Cloud-enabled Management troubleshooting and maintenance tasks”](#) on page 272.

Configuring a site server communication profile

The site server communication profile defines the information that the Symantec Management Agents require to establish connection to a site server.

When the site server sends its certificate information to Notification Server, it automatically creates a unique communication profile for this site server.

After the Notification Server creates the communication profile, you can edit it. For example, you can add the proxy settings.

To configure the site server communication profile

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the left pane, expand **Site Management > Site Servers**, expand the site server for which you want to configure the communication profile, and then click **Communication Profile**.
- 3 In the right pane, click the name of the communication profile.
- 4 On the communication profile page, make the necessary changes.
For more information, click the page and then press **F1**.
- 5 Click **Save changes**.

About configuring the site service settings

The site service settings are usually global default settings. Any changes that you make to the settings for a particular site service type are applied to all site services of that type. However, starting from IT Management Suite version 8.0, you can specify and apply individual package service settings to each package server separately. The individual settings override the global settings.

You can view and modify the global settings for each site service. For package service, you can also view and modify the individual settings.

In the left pane, each installed service is shown underneath each site server. The corresponding page shows the service summary for the site server. The panel is expanded by default, rather than collapsed for statistics as on the site server page.

For many services, the summary information that is shown here may be the same as the summary information expandable on the site server page. However, the Symantec Management Platform allows a service to provide a different control in this context, if appropriate. For example, if there is a full page of data available, it is displayed on the site service page. A condensed data set is displayed on the site server page.

See [“Configuring package service settings”](#) on page 113.

See [“Configuring individual package service settings”](#) on page 113.

See [“Configuring task service settings”](#) on page 114.

See topics about monitor service in the *Monitor Solution User Guide*.

Configuring package service settings

You need to configure the global package service settings. These settings are applied to all package services that are installed on site servers in your Symantec Management Platform.

Note that you can also specify and apply individual package service settings to each site server separately. The individual settings override the global settings.

See [“Configuring individual package service settings”](#) on page 113.

To configure package service settings

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the left pane, expand **Site Management > Settings > Package Service** and then click **Package Service Settings**.
- 3 On the **Package Service Settings** page, configure the appropriate settings:

To set the global package service settings

In the **Global Package Service Settings** pane, make the necessary changes.

For more information, click the page and then press **F1**.

To set up unconstrained package servers

In the **Constrained Package Server Selection** pane, set up each package server by checking or unchecking the **Constrained** check box, as appropriate.

You can use the **Site** drop-down list to view the summary information about all the package servers in a specific site, or all sites.

- 4 Click **Save changes**.

Configuring individual package service settings

The package service settings are usually set with the global settings that apply to all package servers. However, you can also specify and apply individual package service settings to package servers. The individual settings override the global settings.

See [“Configuring package service settings”](#) on page 113.

To configure individual package service settings

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the left pane, expand **Site Management > Site Servers**, and then click the server to which you want to apply the individual package service settings.
- 3 In the right pane, expand the **Package Service** panel, and then click the **Change global Package Service settings** link.
- 4 In the **Custom Package Service Settings** dialog box, edit the necessary package service settings, enable the settings, and then click **Save changes**.
- 5 (Optional) On the site server for which you applied the custom package service settings, update the configuration in the Symantec Management Agent.

Configuring task service settings

You can apply task service settings to the task servers that computers, users, or resources use. Notification Server applies these settings to the chosen task services that are installed on the site servers in your environment.

Warning: Make sure that only one **Task Service Settings** policy is applied to each task server. Applying multiple policies to one task server may have unexpected results.

See [“About Task Management”](#) on page 340.

See [“Sequencing tasks”](#) on page 347.

To configure task service settings

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the left pane, expand **Settings > Task Service > Settings**, and then click **Task Service Settings**.
- 3 On the **Task Service Settings** page, configure the appropriate settings.
For more information, click the page and then press **F1**.
- 4 In the **Applied To** panel, click **Apply to** to select the computers, users, or resources to which these task service settings apply.
These settings apply to the task services that these computers, users, or resources use.
- 5 Click **Save changes**.

Configuring Package Server for Linux

This chapter includes the following topics:

- [About package server for Linux](#)
- [About integrating Apache Web Server with package server for Linux](#)
- [About detecting the Apache Web Server](#)
- [Requirements to configure package server and the Apache Web Server](#)
- [Requirements to configure HTTPS and HTTP](#)
- [Package server configuration example that uses main web directory for package server links](#)
- [Package server configuration example using an alias for package server links](#)

About package server for Linux

To designate a Linux computer as a package server, ensure that the computer is running the following software:

- Symantec Management Agent for UNIX, Linux, and Mac
Symantec Management Agent for UNIX, Linux, and Mac runs on a managed computer. That agent must match the version of the agent that is installed on the Notification Server computer in Symantec Management Platform. If the agent on the managed computer is older than the agent on Notification Server, upgrade it. After the agent is upgraded, the managed computer can become a package server.
- Apache Web Server version 2.0 or 2.2
See [“About integrating Apache Web Server with package server for Linux”](#) on page 116.

The following server platforms are supported:

- Red Hat Enterprise Linux Server 6
- Red Hat Enterprise Linux Server 7
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11 SP1, 11 SP2, 11 SP3

Package server for Linux supports alternate download locations. Paths for alternate locations are converted automatically from Windows style to UNIX style if you include the trailing slash. For example, if you have Patch Management Solution installed, you can change policy and package settings when rolling out patches. In Symantec Management Console, under **Settings > All Settings > Software > Patch Management**, you click a vendor settings page; for example, you would click **Red Hat Settings > Red Hat Patch Remediation Settings**. When you click the **Policy and Package Settings** tab, you see the **Remediation Settings** page for the selected product. This is where you can check **Use alternate download location on Package Server**. When you enter the alternate download location, you must use the full Windows path. In this and similar instances, include a trailing slash in the Windows-style path to ensure that it is converted correctly to a UNIX-style path.

Correct: Trailing slash means that the Windows path is converted correctly to
C:\path\ /path/.

Incorrect: If you omit the trailing slash, the Windows path is converted incorrectly.
C:\path

About integrating Apache Web Server with package server for Linux

You integrate package server for Linux with the Apache Web Server to expose packages and Package Snapshots to Symantec Management Agent. Snapshots are downloaded from Notification Server to Symantec Management Agent on all supported platforms through HTTP URLs.

See [“About package server for Linux”](#) on page 115.

The packages and package snapshots are always downloaded to package server directories. The only files that are created in the Apache Web Server are directories, symbolic links, and .htaccess files. Symbolic links are created to the package files and snapshot files. The .htaccess files lock down package files with passwords.

When a Linux computer becomes a package server, the agent on that computer attempts to create an HTTP share in the Apache Web Server virtual web space.

The Package Manifest file is not used when a package server for Linux downloads a package for distribution. The exception is if the package is located in the same directory for the package server for Linux and Software Delivery. All package file permissions are set to allow Apache Web Server clients access. This access is typically through 0x744.

Depending on the specific configuration of the Apache Web Server, directories are created in the root of the web directory. An example is `/var/www/html` on a typical Linux Red Hat system. The package server agent reads the Apache Web Server configuration file to determine this location.

See [“About detecting the Apache Web Server”](#) on page 117.

If you choose, you can specify that package server create the directories in an alternate location. Use an Apache Web Server alias directive to specify a separate directory.

See [“Requirements to configure package server and the Apache Web Server”](#) on page 118.

See [“Requirements to configure HTTPS and HTTP”](#) on page 120.

About detecting the Apache Web Server

You can detect the Apache Web Server automatically or manually.

See [“About integrating Apache Web Server with package server for Linux”](#) on page 116.

See [“Requirements to configure package server and the Apache Web Server”](#) on page 118.

If you choose Automatic Detection, Symantec Management Agent looks for the Apache HTTPD or HTTPD2 executable in the following directory locations:

- `/bin:/usr/bin:/sbin:/usr/sbin:/usr/lbin:/usr/etc:/etc:/usr/bsd:/usr/local/bin:/usr/contrib/bin/`
- System PATH variable
- `/opt/apache/bin:/usr/apache/bin:/usr/apache2/bin:/usr/local/apache/bin:/usr/local/apache2/bin:/usr/local/bin:/opt/freeware/apache/bin:/opt/freeware/apache2/bin:/opt/freeware/apache/sbin:/opt/hpws/apache/bin:/opt/apache2:/usr/local/apache+php`

If both HTTPD and HTTPD2 executables are found, then both Apache 2.0 and Apache 2.2 are installed.

In addition, if both executable files are found, then the file that matches a running process is used. The default file is HTTPD2.

If the Apache Web Server cannot be detected automatically, you may need to detect it manually. The Apache Web Server might not be detected automatically if the executable file is renamed. If multiple installations have occurred, then the wrong Apache Web Server could be detected. In any of these situations, you should specify the Apache Web Server location manually.

To specify the Apache Web Server manually you should edit the **[httpd Integration]** section of the client.conf file in the agent. In this section, you should specify the "apache_exe_location" setting.

When the Apache Web Server executable is located, it is used to determine the default location of the Apache Web Server configuration file. The configuration file is required to determine if the Apache Web Server setup is suitable for package server use. The configuration file also lets the installation program determine the settings that are applicable to the package server. Applicable settings include the ports that are used or whether the server is SSL-enabled.

If Symantec Management Agent for UNIX, Linux, and Mac cannot find the Apache Web Server configuration file, it searches in the following locations:

- /etc/httpd/conf
- /etc/httpd/2.0/conf

As an alternative to Automatic Detection you can edit the **[Httpd Integration]** section of the Symantec Management Agent for UNIX, Linux, and Mac client.conf file. When you edit the file, specify the apache_config_location. Any setting that you change becomes the default.

You can use the Apache Web Server "-f" option during the installation to relocate the configuration file from its default location. If you relocate the file, you must specify the location of the apache_config_location. Package server for Linux does not support mod_perl generated httpd.conf files.

Requirements to configure package server and the Apache Web Server

For the package server for Linux to work with the Apache Web Server, certain requirements must be met. When these requirements are met, the Symantec Management Agent for UNIX, Linux, and Mac sends the Apache HTTP Server role. This role allows the computer to be used as a package server for Linux.

See [“About detecting the Apache Web Server”](#) on page 117.

The configuration requirements are as follows:

- Apache Web Server version 2.0, 2.2, or 2.4 is installed.
- The package server for Linux uses only the main Apache Web Server or the default Apache Web Server.

All other virtual host sections in the Apache Web Server configuration are ignored, with the following exceptions:

- The global settings and the **_default_** virtual host are read for the main server settings.

- The first virtual host that defines an SSL server is considered to be the main SSL server. Its settings are used for integrating and all other SSL virtual hosts are ignored.
- The Apache Web Server web space location where the package server files and directories are to be created must have the following options enabled:
 - **FollowSymLinks**
 - **AllowOverride**
- The usage of HTTP and/or HTTPS for the Apache Web Server depends on the **Published Codebase Types** value defined as part of the **Package Service Settings** for the Notification Server.
- Non-standard ports are detected and used, but the main Apache Web Server must be accessible through the hostname of the computer. The **Listen** directive for the main server must come before all other **Port** statements and Listen directives in the configuration file.
- The Apache Web Server must be running.
- No compressing modules are used with the Apache Web Server. This requirement exists because Package Delivery does not support those modules.
- In SUSE Linux Enterprise 15, you must additionally perform the following configuration for Apache Web Server 2.4:
 - In `/etc/apache2/httpd.conf` file:


```
<Directory />
Options FollowSymLinks
AllowOverride None
</Directory>
```
 - In `/etc/apache2/default-server.conf` file:


```
<Directory "/srv/www/htdocs">
AllowOverride All
<IfModule !mod_access_compat.c>
Require all granted
</IfModule>
<IfModule mod_access_compat.c>
Order allow,deny
Allow from all
</IfModule>
</Directory>
```
- In CentOS 7 and RHEL 7, you must additionally perform the following configuration for Apache Web Server 2.4:
 - In `/etc/httpd/conf/httpd.conf` file:

```
<Directory />
Options FollowSymLinks
AllowOverride None
</Directory>
<Directory "/var/www/html">
Options Indexes FollowSymLinks
AllowOverride All
Order allow,deny
Allow from all
</Directory>
```

- You may need to restart Symantec Management Agent for UNIX, Linux, and Mac after you make changes to the httpd.conf file. The files may not take effect until after you restart the agent.

Requirements to configure HTTPS and HTTP

Symantec Management Agent for UNIX, Linux, and Mac uses whichever type of Apache Web Server is available. It can use either HTTP or HTTPS.

See [“Requirements to configure package server and the Apache Web Server”](#) on page 118.

If the Apache Web Server supports both types of Web server, the package server for Linux uses HTTPS. Integrating with SSL through HTTPS is the default option because it is the most secure. If you want to use the HTTP server, you can change the **[httpd Integration] "integrate_with"** setting.

Table 8-1 Recommended approaches for installing the Apache Web Server to support package servers for UNIX and Linux

Option	Description
Install a packaged version of Apache Web Server. On Linux, the distributed Apache Web Server is most suitable.	This installation contains the executable files and the technical support exe files in /usr/sbin or /usr/bin .

Table 8-1 Recommended approaches for installing the Apache Web Server to support package servers for UNIX and Linux (*continued*)

Option	Description
Install the Apache Web Server package in the recommended location.	An example of a suitable default location is /usr/local or /opt .
Leave the Configuration directory in its default location. This requirement ensures that Symantec Management Agent for UNIX, Linux, and Mac can easily detect the Apache Web Server and the configuration file. If you do not move the configuration directory, you do not have to specify extra manual settings.	The default configuration directory is the location that was compiled into your .exe, or /etc/httpd/conf .

If you change the Apache Web Server configuration files while Symantec Management Agent is running, data is sent to Notification Server after a short time. After the Apache Web Server role data is sent to Notification Server, the computer becomes a candidate package server . If you want to speed up this process you should run the **aex-sendbasicinventory** executable file manually. Run the executable file from the shell on the client computer that is targeted for the package server installation. Update Notification Server with the changes.

Two configuration examples are available.

See [“Package server configuration example that uses main web directory for package server links”](#) on page 121.

See [“Package server configuration example using an alias for package server links”](#) on page 123.

Package server configuration example that uses main web directory for package server links

This configuration generally requires the minimal modification to an out-of-the-box or default Apache Web Server setup. In this configuration a virtual directory that is called **/Altiris/PS** is created automatically under the main Apache HTML directory.

See [“Requirements to configure HTTPS and HTTP”](#) on page 120.

The example configuration contains the **Packages** directory.

Symbolic links are created in these directories to each shared package. The packages themselves are stored under the package server agent **VAR** directory.

This configuration includes both an HTTP and an HTTPS Apache server. The package server uses the HTTPS server if it is available. The HTTPS server ensures a more secure operating environment and allows the use of Package Access credentials.

Several configuration file checks are performed. The configuration files that are listed in this section are examples. These examples are from the default installation of the Apache Web Server as part of a legacy Red Hat Linux Distribution.

Check number 1; Listen statement is as follows:

```
...## When we also provide SSL we have to listen to the ## standard HTTP port
(see above) and to the HTTPS port ## <IfDefine HAVE_SSL> Listen 80 Listen 443
Listen 10.10.10.10:8080 </IfDefine>...
```

Ensure that the Listen statement for each of the main servers is the first Listen statement of its type in the configuration file. The main HTTP and HTTPS servers should be the first two Listen statements.

You should remove the IP or ensure that it is the same IP to which the hostname resolves, as reported to Notification Server.

Check number 2; Main directory options is as follows:

```
...
# DocumentRoot: The directory out of which you will serve your Notification
Server Reference 62

# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
DocumentRoot "/var/www/html" ...

# This should be changed to whatever you set DocumentRoot to.
#<Directory "/var/www/html">

# This may also be "None", "All", or any combination of "Indexes",
# "Includes", "FollowSymLinks", "ExecCGI", or "MultiViews".
# Note that "MultiViews" must be named *explicitly* --- "Options All"
# does not give it to you.
Options Indexes FollowSymLinks

# This controls which options the .htaccess files in directories can
# override. Can also be "All", or any combination of "Options", "FileInfo",
# "AuthConfig", and "Limit" AllowOverride AuthConfig
# Controls who can get stuff from this server.

Order allow,deny

Allow from all
```

```
</Directory>
```

```
...
```

Find the **<Directory>** node for the **DocumentRoot** directory, and ensure that the following options are set:

- **FollowSymLinks**
- **AllowOverride AuthConfig** or **Allow override All**

Check number 3; Check SSL host is as follows:

```
## SSL Virtual Host Context
<VirtualHost _default_:443>
# General setup for the virtual host
DocumentRoot "/var/www/html"
ErrorLog logs/error_log
TransferLog logs/access_log Notification Server Reference 63
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on
...
```

Ensure that the **_default_** SSH Virtual host has the correct port. The port should match the first SSH Listen. Ensure that the DocumentRoot of the virtual host is the same as the DocumentRoot of the main server.

The DocumentRoot of the host can be different from the DocumentRoot of the main server. The DocumentRoot of the host must have a **<Directory>** node that is configured with the same options that are specified in Check number 2.

Package server configuration example using an alias for package server links

You may want to keep the package server for Linux virtual directory completely separate from the Apache Web Server directory. To keep them separate, follow this configuration example. This configuration example keeps all the symbolic links out of the main Apache Web Server directory. It ensures that the FollowSymLinks options are not required in the main directory.

See [“Requirements to configure HTTPS and HTTP”](#) on page 120.

An alias is used in the Apache Web Server configuration file to separate the **/Altiris/ PS** virtual directory. The package server for Linux automatically detects this alias and creates the required subdirectories in the correct location.

The subdirectories are as follows:

- **Packages**
- **Snapshots**

The actual packages are downloaded to the **VAR** directory on the agent.

The configuration files that are used in this section are an example. The example is from the default installation of the Apache Web Server as part of a legacy Red Hat Linux Distribution.

The **Check number 1; Listen statement** is as follows:

```
...## When we also provide SSL we have to listen to the
## standard HTTP port (see above) and to the HTTPS port
##
<IfDefine HAVE_SSL>
Listen 80
Listen 443
Listen 10.10.10.10:8080
</IfDefine>
...
```

Ensure that the Listen statement for each of the main servers is the first Listen statement of its type in the configuration file. The main HTTP and HTTPS servers should be the first two Listen statements.

You should remove the IP or ensure that it is the same IP to which the hostname resolves, as reported to Notification Server. You can use port numbers other than 80 and 443. The package server for Linux detects the ports. However, it always uses the port of the first Listen in the Apache Web Server configuration file.

Check number 2; Create Alias and aliases directory options is as follows:

```
...
# Aliases: Add here as many aliases as you need (no limit). The format is
# Alias fakename realname
#
<IfModule mod_alias.c>
```

```
...
Alias /Altiris/PS /var/altiris/www/ps
<Directory /var/altiris/www/ps >
Options FollowSymLinks
AllowOverride All
</Directory> </IfModule>
# End of aliases.
```

You should perform these steps in the following order:

- Create both the Alias statement and the **<Directory>** node for the destination directory of the alias.
- Ensure that the following options are set on that directory:
 - **FollowSymLinks**
 - **AllowOverride AuthConfig** or **Allow override All**
- Create the destination directory.
- Set the correct permissions on the destination directory to ensure that Apache Web Server clients can download files from there.
- To ensure that the directory works, place a text file in it. Then browse to a URL such as <http://your.server.name/Altiris/PS/testfile.txt>. In this example, your.server.name and testfile.txt are your own server name and the name of the text file that you created.

Check number 3; Check SSL host is as follows:

```
...
## SSL Virtual Host Context
<VirtualHost _default_:443>
# General setup for the virtual host
DocumentRoot "/var/www/html"
ErrorLog logs/error_log
TransferLog logs/access_log
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on
...
```

Ensure that the **_default_** SSH Virtual host has the correct port. It should match the first SSH Listen. Ensure that its DocumentRoot is the same as the DocumentRoot of the main server.

Configuring hierarchy and hierarchy replication

This chapter includes the following topics:

- [About Notification Server hierarchy](#)
- [Hierarchy and replication requirements](#)
- [Implementing Notification Server hierarchy](#)

About Notification Server hierarchy

Hierarchy is a technology designed to reduce the total cost of ownership (TCO) of managing Symantec software and solutions across multiple Notification Servers. Hierarchy reduces the TCO by supplementing the Notification Server system with centralized management capabilities.

If you have multiple Notification Servers, you can use hierarchy to define collections of Notification Servers that share common configuration settings and data.

A hierarchy topology defines the relationships between Notification Servers, which in turn controls how synchronization occurs between adjacent nodes. Also, it defines schedules for synchronization.

A hierarchy topology complies with the following rules:

- Each Notification Server can have zero or one parent.
- Each Notification Server can have zero or more children. Symantec recommends that you have maximum six child Notification Servers per one parent.

Each child Notification Server computer is only aware of its parent and is unaware of other child Notification Servers.

You can manage from both the parent and the child Notification Server computers. If management is done from a parent server, it can apply to all of the child servers and their

managed computers. If management is done from a child server, the task only applies to the child server's managed computers.

See [“Hierarchy and replication requirements”](#) on page 128.

See [“Implementing Notification Server hierarchy”](#) on page 129.

See [“Configuring hierarchy replication rules”](#) on page 134.

Hierarchy and replication requirements

To share or receive common configuration settings and data with multiple Notification Server computers, you must first add the Notification Server computer to a hierarchy. Because Notification Server computers can be managed locally, each Notification Server computer must be added or removed from a hierarchy individually with the appropriate access credentials. Typically, the Symantec Administrator managing the topology design accesses the Notification Server computers in other sites remotely to add them to a hierarchy.

See [“About Notification Server hierarchy”](#) on page 127.

See [“Implementing Notification Server hierarchy”](#) on page 129.

The requirements for configuring the hierarchy or replication are as follows:

- Network traffic must be routable between adjoining Notification Server computers within the hierarchy.
- HTTP/HTTPS traffic must be permitted between adjoining Notification Server computers within the hierarchy.
- If you use self-signed certificates for Notification Server computers, ensure that the trust between those computers is established. To do so, in the **Microsoft Management Console**, in the **Certificates (Local Computer)** store, manually install certificates to **Trusted Root Certification Authority**.
- Trust relationships must exist between adjoining Notification Server computers within the hierarchy, or credentials for the privileged accounts that facilitate trust must be known.
- Each Notification Server computer must be able to resolve the name and the network address of any adjoining Notification Server computers within the hierarchy.
- There must be sufficient bandwidth between Notification Server sites to support package and data replication.
Bandwidth and the hardware that is required depend on the size of your hierarchy topology and the data replicated.
- A site must exist for each Notification Server computer, and must include the subnet that contains Notification Server. The site must also contain a package server (a site server that is running the package service) that serves the Notification Server computer.

If you do not use Deployment Solution, use the task services on Notification Server. If you use Deployment Solution, dedicate a computer to host both the task services and the package services. This computer is called a network boot server. You must have a dedicated network boot server on each Notification Server site. When you use a dedicated task server, you must manually configure site management to restrict all client computers to use the dedicated task server.

See [“About site services”](#) on page 97.

Implementing Notification Server hierarchy

To share or receive common configuration settings and data with multiple Notification Servers, you must add the Notification Server computer to a hierarchy and configure the necessary replication rules.

Table 9-1 Process for implementing Notification Server hierarchy

Step	Action	Description
Step 1	Create the appropriate hierarchical relationships between Notification Servers.	<p>You create a hierarchy by creating a series of parent-to-child and child-to-parent relationships that link together the Notification Server computers in your system.</p> <p>See “Creating and managing hierarchical relationships” on page 130.</p> <p>See “Setting up a hierarchical relationship between two Notification Server computers” on page 133.</p>
Step 2	Create and enable the appropriate replication rules to specify the data to replicate through the hierarchy.	<p>Hierarchy replication of resources and events is configured using replication rules. These rules define the data that you want to replicate to other Notification Servers.</p> <p>See “Configuring hierarchy replication rules” on page 134.</p> <p>If you want to set up custom hierarchy replication for configuration and managements items, specify the appropriate settings.</p> <p>See “Setting up custom hierarchy replication” on page 137.</p> <p>You can monitor the progress of the replication on the Jobs Management page.</p> <p>See “Viewing replication progress report” on page 138.</p>

Table 9-1 Process for implementing Notification Server hierarchy (*continued*)

Step	Action	Description
Step 3	(Optional) Perform manual replication tasks.	<p>The Notification Server computers in a hierarchy are normally synchronized according to the replication schedule that is set up in the replication rules. However, you can manually override the differential replication schedule for your Notification Server and trigger the hierarchy replication rules immediately.</p> <p>See “Overriding the hierarchy differential replication schedule” on page 139.</p> <p>You can manually replicate selected data directly from a Notification Server to all its child Notification Servers without including it in a replication rule. Manual replication is a once-off replication that takes place immediately. You need the have Read permission on the Replicate Now right-click menu item action to perform manual replication.</p> <p>See “Replicating selected data manually” on page 140.</p>
Step 4	(Optional) Set up hierarchy automation policies.	<p>Hierarchy automation policies send email notifications when certain events occur in the hierarchy.</p> <p>See “Setting up a hierarchy automation policy” on page 140.</p>
Step 5	Run a hierarchy report.	<p>You can run a report on any Notification Server in the hierarchy to extract data from its CMDB. Update the summary data before running a hierarchy report.</p> <p>See “Running a hierarchy report” on page 141.</p> <p>See “Updating summary data” on page 142.</p>

See [“About Notification Server hierarchy”](#) on page 127.

See [“Hierarchy and replication requirements”](#) on page 128.

Creating and managing hierarchical relationships

You create a hierarchy by creating a series of parent-to-child and child-to-parent relationships that link together the Notification Server computers in your system. You can add your Notification Server (the one that you are logged into, which may be a remote logon) to a hierarchy as a child of an existing remote Notification Server, or as its parent.

You can add your Notification Server (the one that you are logged on to, which may be a remote logon) to a hierarchy as a child of an existing remote Notification Server computer, or as its parent. To create a hierarchical relationship, you require a Symantec Administrator account (or an account with equivalent privileges) on both computers. To add or remove

Notification Server computers from a hierarchy, you need the **Manage Hierarchy Topology** privilege on the Notification Server computer where the action is carried out.

You can view and configure the Notification Server computer hierarchy using the Symantec Management Console. If you are the Hierarchy administrator, you can see only the parent and children of your Notification Server.

Note that all actions that you take are based on your Notification Server. Right-clicking a Notification Server computer does not perform a remote logon to any remote Notification Server computers. It opens a context menu containing the actions that you can perform on that server, which is different for local and remote computers. A full set of actions is available for the local server, but only a limited set is available for remote servers. Actions such as extracting reports are performed on the appropriate database.

The actions that you can perform on the hierarchy are relative to your Notification Server computer, which is the computer that you are logged on to. If you have the **Manage Hierarchy** privilege on a remote Notification Server computer, you can perform a remote logon to that computer. You can then open the Symantec Management Console, and perform hierarchy configuration relative to that computer.

You can enable or disable hierarchy replication on specific Notification Server computers at any time. For example, you can use this facility to temporarily disable hierarchy replication during maintenance tasks such as solution installation, upgrades, or uninstallation. Disabling the replication on one Notification Server computer does not affect the replication schedule on the other Notification Server computers in the hierarchy. However, no data is passed through the disabled computer, so replication down stops at the parent, and replication up stops at the children.

A colored symbol on the **Hierarchy Management** page indicates any hierarchy alerts. The colors that you might see and the corresponding alert status are as follows:

Yellow	Low alert status.
Orange	Medium alert status.
Red	Critical alert status.

For example, if you attempt to replicate the same data both up and down the hierarchy from the same Notification Server computer, a critical alert is raised. Data should be replicated one way only. If the parent or the child Notification Server computer has the same hierarchy replication rules implemented, or you could set up a data clash.

This task is a step in the process for implementing Notification Server hierarchy.

See [“Implementing Notification Server hierarchy”](#) on page 129.

To create and manage hierarchical relationships

1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Hierarchy**.

2 On the **Hierarchy Management** page, on the **Topology** tab, perform any of the following tasks:

Add a new Notification Server to a hierarchy See [“Setting up a hierarchical relationship between two Notification Server computers”](#) on page 133.

Modify a hierarchical relationship between two Notification Servers See [“Setting up a hierarchical relationship between two Notification Server computers”](#) on page 133.

Enable or disable hierarchy replication You may want to disable hierarchy participation when you perform maintenance on a Notification Server.

Right-click the Notification Server computer on which you want to enable or disable hierarchy replication, and click **Enable Replication** or **Disable Replication**.

Disabling hierarchy replication affects the hierarchy replication schedule only. It has no effect on any stand-alone replication that has been set up to or from another Notification Server.

Manually synchronizing the hierarchy does not change this setting, but overrides it to perform a once-only replication of the appropriate items.

Manually override the hierarchy replication schedule for a Notification Server See [“Overriding the hierarchy differential replication schedule”](#) on page 139.

Run a hierarchy report Right-click the Notification Server computer for which you want to check the report, click **Reports**, and then click the report that you want to view.

See [“Running a hierarchy report”](#) on page 141.

Remove a Notification Server from the hierarchy Right-click the Notification Server computer that you want to remove, and then click **Remove**.

3 Click **Save changes**.

See [“About Notification Server hierarchy”](#) on page 127.

See [“Hierarchy and replication requirements”](#) on page 128.

Setting up a hierarchical relationship between two Notification Server computers

You can set up a hierarchical relationship (either Parent of or Child of) between your Notification Server computer and a remote Notification Server computer. You need to specify the name, URL (which should include any non-default port configurations or HTTPS), and access details of the remote Notification Server computer. You also need to provide the access details of your local Notification Server computer. By default, the hierarchy replication schedule staggers the replication between each pair of Notification Server computers. You can change the replication schedule to suit your requirements, but you should ensure that replication staggering is maintained.

Both Notification Server computers must have a package server available within their respective sites. The package server is required for performance reasons. You cannot create a hierarchical relationship between two Notification Server computers if either one does not have a package server available.

Notification Server application credentials should be stable and not be changed regularly like some user account passwords. If the Notification Server computer application account password becomes invalid, a message is displayed in the console. The message prompts you to use the AexConfig command-line tool to make the necessary updates.

This task is a step in the process for implementing Notification Server hierarchy.

See [“Implementing Notification Server hierarchy”](#) on page 129.

To set up a hierarchical relationship between two Notification Server computers

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server Management > Hierarchy**.
- 2 On the **Hierarchy Management** page, on the **Topology** tab, right-click your Notification Server, and then click the appropriate option:
 - **Add > Parent**
 - **Add > Child**
- 3 In the **Add Hierarchy Node Wizard**, on the **Notification Server** page, enter the name, URL, and access credentials of the remote Notification Server computer.

The access credentials must be a Symantec Administrator account or equivalent account on the remote Notification Server computer.
- 4 Click **Advanced**.
- 5 In the **Return Credential Setting** dialog box, specify the Symantec Administrator (or equivalent) account that the remote Notification Server computer uses to communicate with the local Notification Server computer, and then click **OK**.
- 6 In the **Add Hierarchy Node Wizard**, click **Next**.

- 7 On the **Replication Schedules** page, set up the differential and the complete replication schedules, and enable those that you want to use on the Notification Server computer, and then click **Next**.

By default, only the differential replication schedule is enabled. Complete replication is rarely used because it puts a heavy load on the Notification Server computer, but you can enable it when necessary. You should schedule the replication at the times that do not clash with replication schedules on other Notification Server computers in the hierarchy.

See [“Managing shared schedules”](#) on page 93.

See [“Configuring a schedule”](#) on page 94.

- 8 On the **Confirm Settings** page, verify that the settings are correct, and then click **Finish**.

The local Notification Server computer uses the specified information to locate and verify the remote Notification Server computer and set up the appropriate hierarchical relationship with it.

If the remote Notification Server computer does not have a package server available within its site, the verification fails and the hierarchical relationship cannot be established.

See [“About Notification Server hierarchy”](#) on page 127.

See [“Hierarchy and replication requirements”](#) on page 128.

Configuring hierarchy replication rules

Hierarchy replication of resources and events is configured using replication rules. These rules define the data that you want to replicate to other Notification Servers. Each rule replicates the specified data in one direction only, up to the parent Notification Server or down to the child Notification Servers. If you set up two rules that have the same resource type being replicated in both directions, a critical alert is raised and the replication rules do not run.

Any data that is replicated down from a parent Notification Server has priority, and overwrites the corresponding data on its child servers. The replicated configuration and management items received from a parent server are usually read-only so they cannot be modified. The read-only setting ensures that it is replicated unchanged down the hierarchy. If you want to allow additions to replicated items on child servers, you need to unlock the relevant items on the Notification Server computer on which they were created. For example, you may want to allow policies to be enabled and disabled on the child Notification Servers.

You may include resource targets in a resource replication rule. Resource scoping applies to the contents (resources) of the targets that are replicated. Therefore, the resources that are replicated depend on the owner of the resource target. The Notification Server administrator can choose to replicate resource targets in their current state (owned by somebody else, with the corresponding scope). Alternatively, they can take ownership of the targets, save them with the administrator’s scope (which usually contains more resources) and replicate them in that state. All the current members of a resource target are replicated. The actual resource

target item is replicated in the background as a dependent item. For example, when a replication rule is created at the parent which applies to a resource target. The resource target is replicated as a dependent item when the replication rule itself replicates down the hierarchy.

Hierarchy has two modes of replication:

Differential Replicates the objects and the data that have changed since the last replication. This mode is enabled by default and reduces the load and the bandwidth that hierarchy uses.

Complete Replicates all objects and data. This mode is disabled by default.

To minimize the load on the network and to prevent data collisions, you should schedule hierarchy replication at a different time for each Notification Server in your hierarchy.

See [“Configuring a schedule”](#) on page 94.

Hierarchy replication synchronizes different types of objects in the following ways:

Configuration and Management Items Policies, tasks, filters, and reports are replicated down the hierarchy. Items use differential replication, which is handled by hashing each item to check for changes and replicating those that have changed.

See [“About running tasks in hierarchy”](#) on page 345.

Note: Server Jobs are not replicated from parent Notification Server to child Notification Servers.

Security Settings Security roles, privileges, and permissions are replicated down the hierarchy. Security objects, such as roles and privileges, always use complete replication.

Resources	<p>Resource information, such as computers, users, sites, and their associated data classes are replicated up or down the hierarchy.</p> <p>Note: If, on parent Notification Server, you manually assign a primary user to a computer, the association is only replicated down the hierarchy. Note that this association can only be changed on parent Notification Server.</p> <p>Resources use differential replication. Differential replication is based on the "last changed" timestamp on the source data. Any data that has changed since the last replication is replicated to the destination server. The data on the destination is then verified, if data verification has been enabled in the appropriate replication rule.</p> <p>Data verification imposes significant processing load on Notification Server. To reduce this load, you can verify a specified percentage of data on the destination server with each replication. For example, if you verify 10% of the data for each replication, that ensures that all data has been verified after 10 replications.</p>
Packages	<p>Packages that are associated with software resources and the data classes that are associated with the packages are replicated down the hierarchy.</p>
Events	<p>Event classes, such as software delivery execution, are replicated up or down the hierarchy.</p> <p>Note that events can overwhelm a parent Notification Server computer when replicated. By default, no events are enabled to replicate. These should be replicated only with great caution and for limited time periods. Note that because replication does not occur real-time, raw event data cannot be used for alerting at the parent Notification Server computer.</p>

This task is a step in the process for implementing Notification Server hierarchy.

See [“Implementing Notification Server hierarchy”](#) on page 129.

To configure hierarchy replication and hierarchy replication rules

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Hierarchy**.
- 2 On the **Hierarchy Management** page, select the **Replication** tab.
- 3 Configure hierarchy replication by selecting the appropriate options.
For more information, click the page and then press **F1**.
- 4 To configure the hierarchy replication rules, do any of the following:

- | | |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create a new hierarchy replication rule | <ol style="list-style-type: none"> 1 Click Add. 2 In the Replication Rule dialog box, specify the appropriate settings.

For more information, click the page and then press F1. 3 Click Save changes. |
| Modify an existing hierarchy replication rule | <ol style="list-style-type: none"> 1 Select the appropriate rule, and then click Edit. 2 In the Replication Rule dialog box, specify the appropriate settings. 3 Click Save changes. |
| Enable a hierarchy replication rule | Check Enabled beside the replication rule name. |
| Delete a hierarchy replication rule | <p>Select the appropriate rule, and then click Delete.</p> <p>The replication rules that are provided with Notification Server or with the installed solutions cannot be deleted. However, you can enable and disable these rules when necessary, and you can edit the rule name and description.</p> |

- 5 Click **Save changes**.

Setting up custom hierarchy replication

You can set up custom hierarchy replication for configuration and management items and security roles and privileges.

The current Item Replication report that you can access from the Configuration and Management Items panel lists all the items that have been enabled for replication using Custom hierarchy replication. When the selected items are replicated, any dependent items that have not been enabled are included automatically. These items do not appear on the Item Replication report. To see a list of all the items that were replicated, you need to view the Objects Replicated report.

This task is a step in the process for implementing Notification Server hierarchy.

See [“Implementing Notification Server hierarchy”](#) on page 129.

To set up custom hierarchy replication for configuration and management items

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Hierarchy**.
- 2 On the **Hierarchy Management** page, on the **Replication** tab, in the **Configuration and Management Items** panel, click **Custom**.

- 3 Click **Save changes**.
- 4 In the Symantec Management Console, in the left pane, right-click on the folder or item that you want to replicate, and then click **Hierarchy > Enable Replication**.
- 5 If you have selected a folder, in the **Inherited Replication Behavior** dialog, specify whether to include the folder contents in the replication:

To include all of the folder contents Click **Yes**.

To replicate only the folder with no contents Click **No**.

If necessary, you can manually enable or disable particular subfolders later.

To set up custom hierarchy replication for security roles and privileges

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Hierarchy**.
- 2 On the **Hierarchy Management** page, on the **Replication** tab, under **Security**, click **Custom**.
- 3 Click **Select security roles and privileges**.
- 4 In the **Select Security Roles and Privileges** window, select the roles and privileges that you want to replicate.
- 5 Click **OK**.
- 6 Click **Save changes**.

Viewing replication progress report

After configuring and starting a replication rule, you can monitor its progress on the **Jobs Management** page.

See [“Configuring standalone replication rules”](#) on page 144.

See [“Configuring hierarchy replication rules”](#) on page 134.

To view replication progress report

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Hierarchy**.
- 2 In the left pane, click **Jobs Management**.
- 3 On the **Jobs Management** page, use the icons on the toolbar to perform the following tasks:

Show detailed information	Shows the detailed information for the selected replication job in a new window. Note: Average transfer speed is viewed as <i>N/A</i> if the transfer time is less than 5 seconds.
Stop selected job	Stops the selected replication job.
Restart selected job	Restarts or resumes the selected replication jobs.
Show source job	Shows the information about the source replication job.

Overriding the hierarchy differential replication schedule

The Notification Server computers in a hierarchy are normally synchronized according to the replication schedule that is set up in the replication rules. If necessary, you can manually override the differential replication schedule for your Notification Server and trigger the hierarchy replication rules immediately. It triggers the hierarchy differential schedule to the selected child node. Any hierarchy replication rules that are set to run on the differential schedule is run immediately. Any rules that are set to run on custom schedules are not triggered to run at the time. You can manually replicate data to your Notification Server from a remote parent or child Notification Server only.

You cannot manually override replication to a remote Notification Server. You can only perform an operation that affects your Notification Server. You can log on to a remote Notification Server to make it your Notification Server, and manually override the differential replication schedules on its parent or its child Notification Servers.

This task is a step in the process for implementing Notification Server hierarchy.

See [“Implementing Notification Server hierarchy”](#) on page 129.

To override the hierarchy differential replication schedule

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Hierarchy**.
- 2 On the **Hierarchy Management** page, on the **Topology** tab, right-click the Notification Server computer from which you want to replicate data.

3 Click **Hierarchy > Replicate To...**

This option triggers the hierarchy replication rules that point to the local (currently logged on) Notification Server. You cannot replicate data from the remote Notification Server to any other remote servers.

4 In the confirmation dialog box, click **OK**.

Replicating selected data manually

You can override the replication rules for your Notification Server by performing a manual hierarchy replication of a particular folder or item. Manual replication replicates the selected data to the child Notification Servers immediately. The data is replicated regardless of the replication schedules or whether the data is included in the replication rules.

This task is a step in the process for implementing Notification Server hierarchy.

See [“Implementing Notification Server hierarchy”](#) on page 129.

To manually replicate selected data from your Notification Server

1 In the Symantec Management Console, in the left pane, right-click the folder or item that you want to replicate.

If you select a folder, the replication includes all of its content (all levels of subfolders and items that it contains). Any parent folders (but not their contents) are also replicated to preserve the folder paths within the structure.

2 Click **Hierarchy > Replicate Now...**

3 In the confirmation dialog box, click **OK**.

Setting up a hierarchy automation policy

Hierarchy automation policies send email notifications when certain events occur in the hierarchy. You need to turn on the policies that you want to use. Note that you cannot modify the default policies, but you may clone them to create new policies. You can then configure those policies to suit your requirements.

This task is a step in the process for implementing Notification Server hierarchy.

See [“Implementing Notification Server hierarchy”](#) on page 129.

To set up a hierarchy automation policy

- 1 In the Symantec Management Console, on the **Manage** menu, click **Automation Policies**.
- 2 In the left pane, click one of the following policies:

Hierarchy Critical Alerts	Sends a high-priority email alert to the Notification System administrator whenever a critical alert is received at the local Notification Server. Critical alert states are also indicated in the Topology tab in the Hierarchy Management page.
Hierarchy Enabling/Disabling	Sends a high-priority email alert to the Notification System administrator whenever hierarchy replication has been enabled or disabled on the local Notification Server.
Hierarchy High Alerts	Sends a high-priority email alert to the Notification System administrator whenever a high alert is received at the local Notification Server.
Hierarchy Structure Change	Sends a high-priority email alert to the Notification System administrator whenever a Notification Server is added to or removed from the hierarchy.

- 3 In the right pane, specify the settings of the policy, and then click **Save changes**.
- 4 On the toolbar, click **Turn on**.

Running a hierarchy report

You can run a report on any Notification Server in the hierarchy to extract data from its CMDB. You may want to update the summary data before running a hierarchy report. You can update the summary data on demand or schedule updates.

See [“Updating summary data”](#) on page 142.

Some installed solutions may supply hierarchy federated reports. These reports summarize the relevant data across the hierarchy, and the results contain a single line for each Notification Server. You can run the full report on a particular Notification Server by double-clicking on the appropriate line.

This task is a step in the process for implementing Notification Server hierarchy.

See [“Implementing Notification Server hierarchy”](#) on page 129.

To run a hierarchy report

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Hierarchy**.
- 2 On the **Hierarchy Management** page, on the **Topology** tab, right-click the Notification Server computer on which you want to run a report.

- 3 Click **Reports** and click the appropriate report.
- 4 On the report page, specify any parameters that you want to use, and refresh the report.
See [“Extracting Notification Server report results”](#) on page 369.

Updating summary data

If you need to generate data for hierarchy-enabled reports, you can update summary data in task server. You can update summary data on demand, schedule a one-time update, or create a custom schedule for recurring updates.

A default schedule runs the task automatically every day. If you want daily updates of the inventory data, you do not need to change the update schedule.

This task is a step in the process for implementing Notification Server hierarchy.

See [“Implementing Notification Server hierarchy”](#) on page 129.

To update summary data on demand

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Notification Server > Task Settings > Update Summary Data**.
- 3 On the **Update Summary Data** page, right-click the task that you want to run, and click **Start Now**.

You can click **Details** to view more information about the task before you run it.

- 4 If the schedule that you want to run is not in the list, create a custom schedule.

To create a schedule

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Notification Server > Task Settings > Update Summary Data**.
- 3 On the **Update Summary Data** page, click **New Schedule**.
- 4 In the **New Schedule** dialog box, specify the settings of the schedule, and then click **Schedule**.

For more information, click the page and then press **F1**.

See [“Running a hierarchy report”](#) on page 141.

Configuring standalone replication rules

This chapter includes the following topics:

- [About standalone replication rules](#)
- [Configuring standalone replication rules](#)
- [Managing replication servers](#)

About standalone replication rules

Replication using the standalone replication rules is a one-way transfer of data between two Notification Servers.

The following replication types are supported:

Differential	Replicates the objects and the data that have changed since the last replication. This method is the recommended method because it reduces the network load and bandwidth consumption when data is replicated.
Complete	Replicates all objects and data. This method is commonly used for hierarchy replication. A complete replication is typically performed monthly to ensure full replication.

To configure replication, you need to set up the appropriate replication rules on each Notification Server computer. Each rule specifies the data to replicate from that server (the source server) to one or more specified destination servers and the schedule to use.

See [“Configuring standalone replication rules”](#) on page 144.

You can create the standalone replication rules for the following items:

Events	Replicates Notification Server events.
Items	Replicates Notification Server configuration items and management items such as tasks, policies, filters, and reports.
Resources	<p>Replicates Notification Server resource types, resource targets, and specific data classes.</p> <p>If you include resource targets in a resource replication rule, remember that resource scoping applies to the contents (resources) of the replicated target. Therefore, the resources that are replicated depend on the owner of the resource target. The Notification Server administrator can choose to replicate resource targets in their current state (owned by somebody else, with the corresponding scope). Alternatively, they can take ownership of the targets, save them with the administrator's scope (which usually contains more resources) and replicate them in that state. All the current members of a resource target are replicated. The actual resource target item is replicated in the background as a dependent item. The target that is applied to a stand-alone rule is replicated when the stand-alone rule itself is replicated. When the rule is run, the target is not sent.</p>
Security	<p>Replicates Notification Server security roles and privileges. Two types of security replication rules are available: Privilege and Role. The configuration procedure is identical for each.</p> <p>When you include a security role in a replication rule, you must also configure a replication rule to replicate all of the privileges in the role. The replicated security role does not recognize any privileges that already exist on the destination Notification Server computer.</p>

Note: Standalone replication of packages is not supported between two Notification Servers with the same version.

Configuring standalone replication rules

Before you start replicating data from one Notification Server to another, you need to plan your replication. This is to ensure that similar data is not passed in both directions. If any of your servers are part of a hierarchy, you need to ensure that the replication does not conflict with the hierarchy replication process. Notification Server does not check to ensure that your replication configuration is consistent with the hierarchy. A poorly planned implementation may create data clashes or overwrites in the affected CMDB-s.

See [“About standalone replication rules”](#) on page 143.

See [“Hierarchy and replication requirements”](#) on page 128.

The rule must be enabled for the specified replication to take place. You can enable and disable replication rules at any time, according to the needs of your organization. For each rule that is enabled, the specified data is replicated according to the defined schedule.

You can replicate data at any time by running the appropriate replication rules. In the console, right-click the rule, and then click **Run**. Running a replication rule overrides its schedule and replicates the specified data to the destination servers immediately. Running a replication rule is a once-only operation and does not change the replication schedule. All replication rules continue to be run as scheduled.

During the replication, all dependencies of the selected items are replicated. For example, if you replicate a task, its schedule, target, and other dependencies are also replicated.

Note: Standalone replication of packages is not supported between two Notification Servers with the same version.

Note: Starting from IT Management Suite version 8.0 HF4, standalone replication is supported between Notification Servers that have different versions of IT Management Suite installed. For more information about replicating data between Notification Servers that have different versions of IT Management Suite installed, see the *IT Management Suite Data Migration Guide*.

To configure a standalone replication rule

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Hierarchy**.
- 2 In the left pane, expand **Replication**.

Note that the replication rules are stored in separate folders based on the data type that they replicate.

Do any of the following:

- | | |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create a new replication rule | <ol style="list-style-type: none">1 Right-click the appropriate folder and click New > Replication Rule.2 On the New replication rule page, specify the appropriate settings. |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

For more information, click the page and then press **F1**.

Modify an existing replication rule	Expand the appropriate folder, and then select the replication rule that you want to modify.
-------------------------------------	----------------------------------------------------------------------------------------------

Enable or disable a replication rule

Expand the appropriate folder, and then right-click the replication rule and click **Enable** or **Disable**, whichever is appropriate.

You can also enable or disable a rule on the **Replication Rule** page, by clicking the rule status (On/Off) icon to toggle the setting.

Run a replication rule

Expand the appropriate folder, right-click the replication rule that you want to run, and then click **Run**.

You can monitor the progress of the replication on the **Jobs Management** page.

See "[Viewing replication progress report](#)" on page 138.

3 Click **Save changes**.

Managing replication servers

The **Servers** page lets you view and manage the standalone replication servers in your environment.

See "[About standalone replication rules](#)" on page 143.

To manage replication servers

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Hierarchy**.
- 2 In the left pane, click **Servers**.
- 3 On the **Servers** page, perform any of the following tasks:

Add a new Notification Server You can add a Notification Server by name or browse the network.

Edit a Notification Server

Click the Notification Server computer that you want to edit, and then click **Edit**.

Delete a Notification Serve

Click the Notification Server computer that you want to remove, and then click **Delete**.

Enabling persistent connection

This chapter includes the following topics:

- [About the Symantec Management Agent communication using persistent connection](#)
- [Enabling persistent connection in your environment](#)

About the Symantec Management Agent communication using persistent connection

Persistent connection in IT Management Suite enables real time data transfer from and to Symantec Management Agent and lets you perform tasks on client computers in real time. For example, you can gather inventory on client computers in real time to validate the current hardware or software state.

See [“About Time Critical Management”](#) on page 41.

Persistent connection in IT Management Suite uses a WebSocket communication protocol. WebSocket operates over HTTPS and uses standard HTTPS port (443) for communication. It does not require keeping additional ports open on the servers or on the client computers. It also uses existing SSL certificates for communication.

Persistent connection supports all applicable settings that are configured in the communication profile. For example, persistent connection uses proxy settings and alternative HTTPS hostname settings if they are configured in a communication profile.

All IT Management Suite infrastructure components (including Internet gateway and remote Task Server) support persistent connection. Also, Windows (Windows 7 and above, Windows Server 2008 and above), Mac, and Linux agents support persistent connection.

When the persistent connection is enabled, all Symantec Management Agents regardless of their location (intranet and Internet) use persistent connection for communicating with Notification Server and site servers.

See [“Enabling persistent connection in your environment”](#) on page 148.

When the persistent connection is enabled for Notification Server, site servers and all required agents, it is used for all management traffic: registrations, sending NSEs, policy downloads, etc. Note that the WebSocket protocol is not used for package downloads.

If persistent connection is disabled or terminated by an intermediate hardware, the communication reverts to using legacy HTTP or HTTPS protocols.

Enabling persistent connection in your environment

Persistent connection in IT Management Suite enables real time data transfer from and to Symantec Management Agent and lets you perform tasks on client computers in real time.

See [“About the Symantec Management Agent communication using persistent connection”](#) on page 147.

The process of enabling persistent connection involves configuring Notification Server, sites servers, and communication profiles for Symantec Management Agents and site servers.

Note: To enable persistent connection, you must have HTTPS set up in your environment.

Table 11-1 Process for enabling persistent connection

Step	Action	Description
Step 1	Enable persistent connection for Notification Server.	You can enable the persistent connection for Notification Server on the Notification Server Settings page, on the Processing tab, under Time Critical Management . See “Configuring Notification Server settings” on page 47.
Step 2	Enable persistent connection for Symantec Management Agents.	After enabling persistent connection for Notification Server, you must configure and enable persistent connection for Symantec Management Agents in the Notification Server communication profile(s). See “Configuring a Notification Server communication profile” on page 247.

Table 11-1 Process for enabling persistent connection (*continued*)

Step	Action	Description
Step 3	Enable persistent connection between site server and Symantec Management Agents.	<p>Ability to enable persistent connection on site servers provides configuration flexibility that takes into account business requirements or specific network limitations of sites and subnets.</p> <p>To enable persistent connection between site servers and Symantec Management Agents, perform the following tasks:</p> <ol style="list-style-type: none"> 1 Enable the Persistent Connection option and specify a port for HTTPS binding on the Global Site Server Settings page. The persistent connection then starts working on this port. <p>Warning: If the Configure HTTPS binding option is unchecked and the HTTPS port is not specified, the WebSocket server does not start on the site server and the persistent connection will not be available.</p> <p>See “Configuring global site server settings” on page 109.</p> <p>Note that you can also configure the settings for each site server individually.</p> <p>See “Configuring individual connection settings for a site server” on page 110.</p> 2 After you configure the site server settings, you must configure and enable the persistent connection in the site server communication profile(s). <p>See “Configuring a site server communication profile” on page 112.</p>

Table 11-1 Process for enabling persistent connection (*continued*)

Step	Action	Description
Step 4	Check the connection status of the agents.	<p>You can check the connection status of the client computers in the following ways:</p> <ul style="list-style-type: none"> ■ In the Symantec Management Console, at Reports > Notification Server Management > Agent, the Agent Connection Status report displays the list of all managed client computers and their connection status. ■ On a client computer, in the Symantec Management Agent UI, on the Agent Settings tab, under Network Status, the Server Connection value shows if the agent uses persistent or non-persistent connection.

Configuring Symantec Endpoint Management Workspaces

This chapter includes the following topics:

- [Preparing Symantec Endpoint Management Workspaces for usage](#)

Preparing Symantec Endpoint Management Workspaces for usage

Before the users can perform any tasks in the Symantec Endpoint Management Workspaces, you need to prepare the appropriate role and permissions and set up the quick tasks.

See [“About Symantec Endpoint Management Workspaces”](#) on page 39.

Table 12-1 Process for preparing Symantec Endpoint Management Workspaces for usage

Step	Action	Description
Step 1	Configure access for the users.	<p>To make the Symantec Endpoint Management Workspaces available to the users, you need to create a new user account (or use an existing one) and add the Endpoint Management Workspaces Users role to it.</p> <p>By default, the Endpoint Management Workspaces Users role has the permission to search for resources and view selected resource details and perform Quick Tasks.</p> <p>See “Configuring access to Symantec Endpoint Management Workspaces” on page 153.</p>
Step 2	Configure the Search scope.	<p>You can control what resources the users can view and search for in the Symantec Endpoint Management Workspaces.</p> <p>Create and populate an organizational view or group and grant read permission to the Endpoint Management Workspaces Users role.</p> <p>See “Configuring search scope for endpoints in Endpoint Management Workspaces” on page 154.</p>
Step 3	Configure access to Targets	<p>Starting from IT Management Suite 8.5 RU2 you can provide the ability for users to search for targets and run quick tasks on them.</p> <p>Create a new target in Symantec Management Console or use an existing one and configure the scoping for the Endpoint Management Workspaces Users role.</p> <p>See “Configuring access to Targets in Endpoint Management Workspaces” on page 155.</p>
Step 4	Set up the Deliver Software quick task.	<p>You can provide the ability for the users to deliver software to one or more endpoints.</p> <p>Create a managed software delivery or a Quick Delivery task and grant read permission to the Endpoint Management Workspaces Users role.</p> <p>See “Setting up the Deliver Software quick task” on page 156.</p>

Table 12-1 Process for preparing Symantec Endpoint Management Workspaces for usage
(continued)

Step	Action	Description
Step 5	Set up the Run Task quick task.	You can provide the ability for the users to run client tasks on one or more endpoints. Create tasks and grant read permissions to the Endpoint Management Workspaces Users role. See “Setting up the Run Task quick task” on page 157.
Step 6	Set up the Reports quick task.	Starting from IT Management Suite 8.5 RU1 you can provide the ability for users to run and view Notification Server reports in the Symantec Endpoint Management Workspaces. See “Setting up the Reports quick task” on page 158.
Step 7	Set up the Change Asset Status quick task	Starting from IT Management Suite 8.5 RU1 you can provide the ability for users to update asset statuses on endpoints in the Symantec Endpoint Management Workspaces. See “Setting up the Change Asset Status quick task” on page 159.

Configuring access to Symantec Endpoint Management Workspaces

To make the Symantec Endpoint Management Workspaces widgets available to the users, you need to create a new user account (or use an existing one) and add the **Endpoint Management Workspaces Users** role to it.

See [“Creating and configuring Symantec Management Platform user accounts”](#) on page 191.

See [“Adding members to a security role”](#) on page 75.

By default, the **Endpoint Management Workspaces Users** role has the permission to search for resources, view selected resource details and perform **Quick Tasks**.

You can edit the role permissions according to your needs. For example, you can leave the permission to run tasks on endpoints and remove all other permissions. In that case, in the Symantec Endpoint Management Workspaces, the user can only see and use the **Run Task** widget in the **Quick Tasks** workspace.

To edit Endpoint Management Workspaces Users role permissions

- 1 In the Symantec Management Console, on the **Settings** menu, click **Security > Security Role Manager**.
- 2 In the Security Role Manager, in the **Role** drop-down list, select the **Endpoint Management Workspaces Users** role.
- 3 In the **View** drop-down list, select **All Items**. To see all items, click the **Show Hidden Items** icon on the toolbar.
- 4 In the left pane expand **Workspaces > Widgets and Workspaces**.
- 5 Click any **Widgets** or **Workspaces** item and make the appropriate changes in the right pane, in the **Item Permissions** panel.
- 6 Click **Save changes**.

If your organization already has a specific role configured for help desk workers, you can add the **Endpoint Management Workspaces Users** role to it so that the help desk workers have the required permissions to work in the Symantec Endpoint Management Workspaces.

To add Endpoint Management Workspaces Users role to an existing security role

- 1 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 2 In the left pane, click **Account Management > Roles**.
- 3 On the **Roles** page, in the left pane, click the security role to which you want to add the **Endpoint Management Workspaces Users** role.
- 4 In the right pane, on the **Members** tab, click **Add Member** and then, click **Add Role**.
- 5 In the **Select Role(s)** dialog box, select the **Endpoint Management Workspaces Users** role, and then click **OK**.
- 6 On the **Members** tab, verify that the list of members is correct. You can remove any that you do not want.
- 7 Click **Save changes**.

See [“Preparing Symantec Endpoint Management Workspaces for usage”](#) on page 151.

Configuring search scope for endpoints in Endpoint Management Workspaces

You can control what resources the users can view and search for by assigning a read permission to an organizational group.

Create and populate an organizational view or group and grant read permission to the **Endpoint Management Workspaces Users** role.

After you grant read permission for an organizational group, the user can view computers (endpoints), that are included to this organizational group and run quick tasks on them in the Symantec Endpoint Management Workspaces.

This task is a step in the process for preparing Symantec Endpoint Management Workspaces for usage.

See [“Preparing Symantec Endpoint Management Workspaces for usage”](#) on page 151.

To configure access to endpoints in Endpoint Management Workspaces

- 1 In the Symantec Management Console, on the **Manage** menu, click **Computers**.
- 2 In the navigation pane, under **Computer Views and Groups**, right-click, and then click **New Organizational View**.
- 3 In the **Organizational View** dialog box, type the name for the organizational view, and then click **OK**.
- 4 Right-click the new organizational view, and then click **New > Organizational Group**.
Note that you cannot add organizational groups to the default **All computers** organizational view
- 5 In the **Organizational Group** dialog box, type the name for the new group, and then click **OK**.
- 6 Under **Computer Views and Groups**, click **All Computers**, and then, in the content pane, select the computers that you want to add to this organizational group.
- 7 To add the selected computers to the organizational group, do one of the following:
 - Drag and drop the selected computers to the organizational group, and then, in the **Add to group** dialog box, click **OK**.
 - Right-click the selected computers, and then click **Add to organizational group**. In the **Add to organizational group** dialog box, click the group that you want to add the computers to, and then click **OK**
- 8 Right-click the new organizational group, and then click **Manage security > Grant Read Permission**.
- 9 In the **Grant Read permission** dialog box, select the **Endpoint Management Workspaces Users** role, and then click **OK**.

Configuring access to Targets in Endpoint Management Workspaces

Starting from Symantec IT Management Suite 8.5 RU2 you can configure access to targets in Endpoint Management Workspaces. After you grant access to a target, the user can see it in the search results and run quick tasks on this target.

Note: Before you proceed with this task, make sure that the **Endpoint Management Workspaces Users** role has read permission to at least one organizational group.

See [“Configuring search scope for endpoints in Endpoint Management Workspaces”](#) on page 154.

You can configure access to existing targets or create new targets in the Symantec Management Console.

See [“Creating or modifying a resource target”](#) on page 323.

This task is a step in the process for preparing Symantec Endpoint Management Workspaces for usage.

See [“Preparing Symantec Endpoint Management Workspaces for usage”](#) on page 151.

To configure access to targets Endpoint Management Workspaces

- 1 In the Symantec Management Console, on the **Manage** menu, click **Computers**.
- 2 In the navigation pane, expand the **Targets** section, click a target, and then, in the content pane, click the **Scoping** link.
- 3 In the **Select scoping roles** dialog box, under **Available resources**, select the **Endpoint Management Workspaces Users** role and click ok.

Note that only the user account that is a member of all selected security roles has full access to the target.. For example, if **Endpoint Management Workspaces Users** and **Level 2 Workers** roles are selected for scoping, the user must be member of both roles to have access to the target in the Endpoint Management Workspaces. Also, the targets only contain the resources (endpoints) that are accessible to the members of the selected roles.

Setting up the Deliver Software quick task

You can provide the ability for the users to deliver software to one or more endpoints.

Note: Before you proceed with this task, make sure that the **Endpoint Management Workspaces Users** role has read permission to at least one organizational group.

See [“Configuring search scope for endpoints in Endpoint Management Workspaces”](#) on page 154.

Create a Managed Software Delivery policy or a Quick Delivery task and grant read permission to the **Endpoint Management Workspaces Users** role.

Quick Delivery is an ideal way for non-administrators, such as help desk personnel, to deliver a single software resource safely and accurately.

Managed Software Delivery is a policy-based delivery method that lets you fulfill advanced delivery requirements. A single Managed Software Delivery policy can perform multiple delivery actions like delivery on a recurring schedule or software installation that replaces other software.

For more information, see topics about software delivery in the *Software Management Solution User Guide*.

After you grant read permission for a Managed Software Delivery policy or a Quick Delivery task, the user is able to view and run this policy or task in the **Deliver Software** widget on the **Quick Tasks** workspace in the Symantec Endpoint Management Workspaces.

This task is a step in the process for preparing Symantec Endpoint Management Workspaces for usage.

See [“Preparing Symantec Endpoint Management Workspaces for usage”](#) on page 151.

To set up the Deliver Software quick task

- 1 In the Symantec Management Console, create a Managed Software Delivery policy or a Quick Delivery task.

Starting from IT Management Suite 8.5 RU2, the Quick Delivery task in Endpoint Management Workspaces ignores all maintenance windows that are specified in Notification Server configuration policies. When the user selects this task in the **Deliver Software** widget, the task runs ASAP. For Managed Software Delivery policy you can configure a specific schedule or allow it to run during a maintenance window.

For more information, see topics about software delivery in the *Software Management Solution User Guide*.

- 2 Right-click the new software delivery policy or Quick Delivery task, and then click **Manage security > Grant Read Permission**.
- 3 In the **Grant Read permission** dialog box, select the **Endpoint Management Workspaces Users** role, and then click **OK**.

Setting up the Run Task quick task

You can provide the ability for the users to run client tasks on one or more endpoints.

Note: Before you proceed with this task, make sure that the **Endpoint Management Workspaces Users** role has read permission to at least one organizational group.

See [“Configuring search scope for endpoints in Endpoint Management Workspaces”](#) on page 154.

Create tasks and grant read permissions to the **Endpoint Management Workspaces Users** role.

After you grant read permission for a task, the user is able to view and run this task in the **Run Task** widget on the **Quick Tasks** workspace in the Symantec Endpoint Management Workspaces. Starting from IT Management Suite 8.5 RU2, the tasks in Endpoint Management Workspaces ignore all maintenance windows that are specified in Notification Server configuration policies. When the user selects a task in the **Run Task** widget, the task runs ASAP.

This task is a step in the process for preparing Symantec Endpoint Management Workspaces for usage.

See [“Preparing Symantec Endpoint Management Workspaces for usage”](#) on page 151.

To set up the **Run Task** quick task

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, right-click the folder where you want to create the task, and then click **New > Task**.
- 3 In the **Create New Task** dialog box, in the left pane, select the task type.

Note: Only **Client Tasks** type tasks can be assigned to **Endpoint Management Workspaces Users** role.

- 4 In the right pane, configure the task.
- 5 Click **OK**.
- 6 Right-click the new task, and then click **Manage security > Grant Read Permission**.
- 7 In the **Grant Read permission** dialog box, select the **Endpoint Management Workspaces Users** role, and then click **OK**.

Setting up the Reports quick task

Starting from IT Management Suite 8.5 RU1 you can provide the ability for users to run and view Notification Server reports in the Symantec Endpoint Management Workspaces.

Note: Before you proceed with this task, make sure that the **Endpoint Management Workspaces Users** role has read permission to at least one organizational group.

See [“Configuring search scope for endpoints in Endpoint Management Workspaces”](#) on page 154.

After you grant read permission for a report, the user is able to run, view, save as a file and print this report in the **Reports** widget on the **Quick Tasks** workspace in the Symantec Endpoint Management Workspaces.

This task is a step in the process for preparing Symantec Endpoint Management Workspaces for usage.

See [“Preparing Symantec Endpoint Management Workspaces for usage”](#) on page 151.

To set up the Reports quick task

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, right-click a report, and then click **Grant Read Permission**.
- 3 In the **Grant Read permission** dialog box, select the **Endpoint Management Workspaces Users** role, and then click **OK**.
- 4 (Optional) Some reports have referenced items (filters, targets, or data sources) for which you also need to add the permission. In the **Add Permissions** dialog box, check the referenced items, associated with the selected report, and click **OK**.

Setting up the Change Asset Status quick task

Starting from IT Management Suite 8.5 RU1 you can provide the ability for users to update asset statuses in the Symantec Endpoint Management Workspaces.

Note: Before you proceed with this task, make sure that the **Endpoint Management Workspaces Users** role has read permission to at least one organizational group.

See [“Configuring search scope for endpoints in Endpoint Management Workspaces”](#) on page 154.

To set up the **Change Asset Status** quick task, create an organizational group and grant read permission for it to the **Endpoint Management Workspaces Users** role. Then add the **Fixed Asset Status Resource Types** to that organizational group.

After you set up this quick task, the user is able to update asset statuses in the **Asset Status** widget on the **Quick Tasks** workspace in the Symantec Endpoint Management Workspaces.

This task is a step in the process for preparing Symantec Endpoint Management Workspaces for usage.

See [“Preparing Symantec Endpoint Management Workspaces for usage”](#) on page 151.

To set up the Asset Status quick task

- 1 In the Symantec Management Console, on the **Manage** menu, click **Organizational Views and Groups**.
- 2 In the left pane, right-click the **Organizational Views** folder and then click **New > Organizational View**.
- 3 Right-click the **New Organizational View** and then click **New > Organizational Group**.

- 4 Right-click the **New Organizational Group** and then click **Manage security > Grant Read Permission**.
- 5 In the **Grant Read permission** dialog box, select the **Endpoint Management Workspaces Users** role, and then click **OK**.
- 6 In the left pane, under **Organizational Views**, click the **Default**.
- 7 In the right pane, at the upper right, click **Filter...**
- 8 In the **Filter Visible Groups** dialog box, check the **Fixed Asset Status Resource Type** and click **OK**.
- 9 In the left pane, expand **Default view > All Resource** and then click **Fixed Asset Status Resource Type**.
- 10 In the right pane, right-click an asset status and click **Add to Organizational Group**.
- 11 In the **Add to Organizational Group** dialog box, select the organizational group that has the **Endpoint Management Workspaces Users** role read permission granted, and then click **OK**.
- 12 (Optional) To add more statuses, repeat step 10 through step 11.

Discovering the resources in your network

- [Chapter 13. Discovering Windows computers](#)
- [Chapter 14. Importing resources from Active Directory](#)
- [Chapter 15. Discovering network devices](#)

Discovering Windows computers

This chapter includes the following topics:

- [Resource discovery methods](#)
- [Discovery methods for Windows computers](#)
- [Discovering computers with domain resource discovery](#)

Resource discovery methods

Discovering all the resources in your network is one of the first steps in successfully managing your network. The Symantec Management Platform provides tools to automatically discover devices in your network. It also creates resources for those discovered in the Configuration Management Database, also known as the CMDB. The ability to automatically discover resources removes the need for time consuming and error prone manual entry.

You can run a manual discovery at any time or you can set up a schedule. By scheduling the discovery, you can automatically create CMDB resources for new computers as they are added to your network.

Table 13-1 Resource discovery methods

Method	Description
Domain resource discovery	<p>If you want to quickly discover Windows computers, you can use domain resource discovery. This method lets you discover the computers that have a trusted account on a domain.</p> <p>When you installed Notification Server, you had the opportunity to use this method to discover computers automatically.</p> <p>See “Discovery methods for Windows computers” on page 163.</p>
Active Directory import	<p>You can import some or all of the resources in your Microsoft Active Directory into the CMDB. You can configure resource import rules to identify and import the resources that you want. You can then configure schedules to perform full imports and update imports at the appropriate intervals.</p> <p>See “Discovery methods for Windows computers” on page 163.</p>
Network Discovery	<p>If you want to discover all resources on all platforms, use Network Discovery. Using Network Discovery, you can discover all IP devices that are connected to your network. You can discover routers, switches, hubs, network printers, Novell NetWare servers, and Windows, UNIX, Linux, and Macintosh computers.</p> <p>See “About Network Discovery” on page 177.</p>

Discovery methods for Windows computers

Before you can manage computers, you must do the following:

- Discover the computers on your network.
- Create resources for them in the CMDB.

This process is called discovery and lets you discover the computers on which you can install the Symantec Management Agent and various solution agent/plugin.

You can discover Windows computers by doing the following:

- Searching for all Windows computers on your network that are registered on a specific domain
- Searching for all Windows computers on your network that match the organizational units that you specify

If you want to discover the computers that are running on other operating systems, you can use Network Discovery.

See [“Resource discovery methods”](#) on page 162.

Table 13-2 Discovery methods for Windows computers

Method	Description
Resource discovery	<p>Searches the specified domain for all computers that are registered on that domain. You must choose at least one of the Domain Browse List or Domain Membership options.</p> <p>See “Discovering computers with domain resource discovery” on page 164.</p>
Microsoft Active Directory Import	<p>Lets you import the computer resources that match the organizational units that you specify. You can also filter the computers that have been active within a specific number of days or that are running a specific Windows operating system.</p> <p>This method returns detailed information on the operating systems for each of your discovered computers and is the preferred method.</p> <p>See “Importing resources using Microsoft Active Directory Import” on page 170.</p>

You can use these discovery methods to discover all your computers in domains, or you can target computers in a single domain.

Discovering computers with domain resource discovery

You can discover Windows computers by searching domain resource information. Discovered computers have a resource created for them in the CMDDB. You can run a discovery manually or use a schedule. After a discovery is run, you can view the reports that show your discovery results.

This database contains the following information on each discovered computer:

- Name (Domain Browse List and Domain Membership)
- OS name (Domain Browse List and Domain Membership)
- Main version (Domain Browse List)
- Minor version (Domain Browse List)
- Platform (Domain Browse List)

See [“Discovery methods for Windows computers”](#) on page 163.

Note: The status message on the **Resource Discovery** page shows the last time that discovery was run manually from the page. The time is not updated to show any subsequent scheduled discovery that has been run.

To discover computers with domain resource discovery

- 1 In the Symantec Management Console, on the **Actions** menu, click **Discover > Import Domain Membership/WINS**.
- 2 On the **Domain Membership/WINS Import** page, under **Domains to search**, type the name of a domain you want to search, and then click the add icon.
- 3 (Optional) To enter a different user name and password for the domain so that Notification Server has access, complete the following steps in order:
 - Select the domain.
 - Click the pencil icon.
 - Click **Use these credentials**.
 - Enter the user name and password, and then click **OK**.
- 4 Select at least one of the following options:

Domain Browse List This method is designed for small, peer-to-peer environments.

The method uses the network browse list to discover all computers on the domain. The browse option discovers all computers that share files or printers or are running the Windows Messenger Service. These computers include Windows NT/2000/2003/2008/95/98/98 SE/ME/XP/7/8.

This method can also discover computers in a workgroup that meet the search criteria.

The Domain Browse List works by enumerating the records in the computer browse list. This computer browse list was designed for a small, peer-to-peer environment, so it does not scale to large environments well.

When Notification Server performs a Domain Browse List discovery, it requests a copy of the computer browse list. The browse list includes additional information such as the computer's operating system and version. It then does a reverse lookup of the computer's name to get its IP address.

You might have problems discovering computers using this method if the following conditions exist:

- The computer is not in the computer browse list.
- The computer is in the computer browse list but not registered as sharing files.
- It can take between 15 minutes and 51 minutes for changes to be reflected in the computer browse list.

The Domain Browse List discovery method gets as much of the computer browse list as it can and as fast as it can. This method can overload a PDC in a large domain or a multi-domain environment. Symantec recommends that you run this outside business hours, preferably over a weekend.

Domain Membership This option discovers all computers with trust accounts in the domain. It can discover computers in Windows NT 4.0 domains or Windows 2000 and later Active Directory domains. This method finds all Windows NT/2000/2003/2008/XP/7/8 computers in the domain. However, any Windows 95/98/98 SE/ME computers are not found.

Note: Limited information can be discovered on computers in NT 4.0 domains. For example, the specific operating system of the computer is not known.

Domain Membership discovery works by enumerating the computer accounts in the specified domains.

When you add a Windows NT/2000/2003/2008/XP/7/8 computer to a domain, a computer account is created in that domain. The computer uses this account to authenticate with the domain so the computer can authenticate user logons using a secure connection. Windows 9x computers do not create a computer account, which is why you cannot find Windows 9x computers using this method.

When discovering computers using the Domain Membership method, Notification Server catalogs these accounts. Unlike the Domain Browse List method, these accounts have no additional information beyond the computer's name. Notification Server still does a reverse lookup on the name to get its IP address.

5 Choose one of the following options:

Discover now Click **Discover Now**.

Set schedule Under **Scheduling Options**, in the **Schedule** drop-down list, specify the schedule of the import.

6 Click **Save changes**.

7 To view the discovery results, do the following:

- Click **View Discovery Reports**.
- In the **Resource Discovery Reports** window, right-click a report and click **Open in New Window**.
- Enter the parameters for the report.
- Click **Refresh**.

Importing resources from Active Directory

This chapter includes the following topics:

- [About Microsoft Active Directory Import](#)
- [About importing resource associations](#)
- [Importing resources using Microsoft Active Directory Import](#)

About Microsoft Active Directory Import

The Microsoft Active Directory Import feature of the Symantec Management Platform lets you import Active Directory objects, such as users, computers, sites, and subnets, into the CMDB. This feature lets you leverage the data that already exists in Active Directory without re-creating it. You can schedule regular imports to keep your CMDB populated with up-to-date resources, allowing better management of your environment.

Microsoft Active Directory Import uses Lightweight Directory Access Protocol (LDAP) to provide one-way synchronization from Active Directory to the Symantec Management Platform. LDAP is the same protocol used by standard Active Directory administration tools. Microsoft Active Directory Import supports Windows 2003 and 2008 domains.

To use Microsoft Active Directory Import, you need to define the appropriate resource import rules to import the resources that you want. You can schedule the resource import rules to run at regular intervals, and you can run them manually at any time. When you run a resource import rule, you can import all of the appropriate data (a full import). Alternatively, you can import the data that is new or changed in Active Directory since the previous import (an update import). As part of the import process, you can automatically create filters or organizational groups based on the organizational units, security groups, and distribution groups that are set up in Active Directory. These filters can be used to specify resource targets to which you apply policies and tasks.

See [“About resource filters”](#) on page 297.

See [“Importing resources using Microsoft Active Directory Import”](#) on page 170.

During the import process, the computers from Active Directory are matched with managed computers in the CMDB, using the computer name and domain. However, Microsoft Active Directory Import imports all computers that the resource import rules identify, regardless of their Symantec Management Agent installation status. Importing all computers lets you import new and unmanaged computers and then target those computers for Symantec Management Agent installation.

Note: You can also discover new and unmanaged Windows computers using Resource Discovery.

See [“Discovery methods for Windows computers”](#) on page 163.

If there are any errors in the import process, you can check the Symantec Management Platform status log for information. The status log can be accessed from the Start menu on the Symantec Management Platform computer: **All Programs > Symantec > Diagnostics > Altiris Log Viewer**.

The Symantec Management Platform includes a number of reports that provide information on Microsoft Active Directory Import activities. These reports are stored in the **Reports > Notification Server Management > Microsoft Active Directory** folder.

About importing resource associations

Microsoft Active Directory not only stores objects, it also stores relationships between objects. Microsoft Active Directory Import can extract these relationships from Active Directory and create the appropriate resources and resource associations in the CMDB. Microsoft Active Directory Import supports four resource associations for users and one resource association between subnets and sites. For the User resource you can also define a new association.

Table 14-1 Resource associations supported by Microsoft Active Directory Import

Resource association	Description
User - Company	Creates a Company resource for the imported User based on its "company" attribute in Active Directory.
User - Department	Creates a Department resource for the imported User based on its "department" attribute in Active Directory.
User - User	Creates one or more User resources for the imported User based on its "directReports" attribute in Active Directory.

Table 14-1 Resource associations supported by Microsoft Active Directory Import
(continued)

Resource association	Description
User - User	Creates a User resource for the imported User based on its "manager" attribute in Active Directory.
Site - Subnet	Creates one or more Subnet resources for the imported Site based on its "siteObjectBL" attribute in Active Directory.
Subnet - Site	Creates a Site resource for the imported Subnet based on its "siteObject" attribute in Active Directory.

The **Enable Resource Associations** window lets you use these relationships in a resource import rule to import other related resources that are not explicitly specified in the rule. By default, all of the available resource associations are enabled.

See [“Creating and modifying resource import rules”](#) on page 171.

Importing resources using Microsoft Active Directory Import

You can import all of the computers that are registered in your Active Directory. Alternatively, you can choose to import only the computers that match the criteria you specify.

See [“About Microsoft Active Directory Import”](#) on page 168.

When you install the Symantec Management Platform, you can use Microsoft Active Directory Import to import all your computers. You can then target the unmanaged computers for Symantec Management Agent installation. Microsoft Active Directory Import is the preferred method for identifying new and unmanaged computers. It returns detailed information on the operating systems for each of your discovered computers.

You can also use Microsoft Active Directory Import to create Symantec Management Platform accounts and roles from Windows users and groups. You import Windows users and groups so that you do not have to manually create Symantec Management Platform accounts and roles. Microsoft Active Directory Import has a resource import rule for importing role and account resources. When this rule runs, it duplicates the Windows user and group structure in Symantec Management Platform. It creates a Symantec Management Platform account for all of the Windows users in the selected security groups. It also creates Symantec Management Platform roles for each of the selected security groups. Finally, it puts the newly created Symantec Management accounts into the Symantec Management Platform roles where the corresponding Windows user is put into the corresponding Windows group.

After the initial import, you can configure resource import the rules that regularly check Active Directory for new or changed resources and then import the appropriate resources to the CMDB.

When you configure resource import rules, you can specify the Active Directory source structure from which to import. You can apply the constraints that filter the imported computers according to your requirements. For example, you can import only the computers that have changed their computer account password within a particular number of days or those that are running a particular Windows operating system.

Table 14-2 Process for importing resources using Microsoft Active Directory Import

Step	Action	Description
Step 1	Configure the appropriate resource import rules.	You can create any new resource import rules that you want and modify the existing rules to suit your requirements. You can also delete any rules that you no longer need. See “Creating and modifying resource import rules” on page 171.
Step 2	Schedule the resource import rules.	For each resource import rule, you can schedule full imports and update imports to run at appropriate intervals. See “Scheduling resource import rules” on page 173.
Step 3	Configure the Directory Synchronization schedule.	The Directory Synchronization schedule identifies previously imported resources that no longer exist in Active Directory and removes them from the CMDB. See “Configuring the Directory Synchronization schedule” on page 175.
Step 4	(Optional) Run a resource import rule manually.	You can run a resource import rule manually at any time. You can run the rule as a full import or an update import. See “Running resource import rules manually” on page 176.

Creating and modifying resource import rules

Resource import rules let you specify the resources that you want to import from Active Directory.

Six default resource import rules are supplied with the Symantec Management Platform, one for each of the supported resource types: User, Computer, Print Queue, Site, Subnet, and Role and Account. You can modify these rules to suit your requirements, or you can create new rules to import the resources that you want.

You can configure a rule to automatically create filters or organizational groups based on the Active Directory organizational units, security groups, and distribution groups from which the

rule imports resources. These filters can then be used to specify resource targets to which you apply policies and tasks.

You can schedule your resource import rules to update the CMDB at regular intervals, or you can run a particular rule manually at any time. Running your resource import rules periodically ensures that any changes to Active Directory are reflected in the CMDB.

This task is a step in the process for importing resources using Microsoft Active Directory Import.

See [“Importing resources using Microsoft Active Directory Import”](#) on page 170.

To create or modify a resource import rule

- 1 In the Symantec Management Console, on the **Actions** menu, click **Discover > Import Microsoft Active Directory**.

- 2 On the **Microsoft Active Directory Import** page, perform one of the following tasks:

To create a new resource import rule	In the toolbar, click Create a new import rule . The new rule is added to the list of resource import rules.
--------------------------------------	------------------------------------------------------------------------------------------------------------------------

To modify an existing resource import rule	In the list of resource import rules, select the appropriate rule.
--------------------------------------------	--------------------------------------------------------------------

To delete a resource import rule	In the list of resource import rules, select the appropriate rule, and then in the toolbar, click Delete the selected import rule .
----------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------

- 3 In the resource import rule that you want to modify, for each of the highlighted links, click the link, and then specify the appropriate settings.

Specified resource type (default setting), Computer, User, Site, Subnet	Specify the domain type and resource type that you want to import and the appropriate Active Directory source structure.
--------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------

Specified data source (default setting)	Specify the domain or server (domain controller) and the appropriate account credentials from which you want to import resources.
------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------

None (default setting) When you click this link, one of the following dialog boxes appears:

- **Select Organizational Unit (OU)**
 Select the Active Directory organizational units or Containers (whichever corresponds to the source structure that you specified in the **Resource Selection** window) from which to import resources. When you select an organizational unit or container, you can choose whether or not to include its descendants.
- **Select Security Groups or Select Distribution Groups**
 Select the particular Active Directory groups from which to import users and groups. The **Select Security Groups** dialog box only appears for the rule that imports role and account resources.

Specified column mappings (default setting), Default column mappings Specify the mapping between the Symantec Management Platform CMDB and Active Directory resource data fields. You can use these mappings to import additional attributes when the Active Directory schema has been extended.

All computers, All users Specify the appropriate criteria to constrain the imported resources to only those that match the specified criteria. A resource is imported only if it meets all of the specified criteria.

These resource associations Specify the resource associations that you want to use to import other related resources that are not explicitly specified in the resource import rule. By default, all of the available resource associations are enabled.

 Microsoft Active Directory Import can extract these relationships from Active Directory and create the appropriate resources and resource associations in the CMDB.

 See [“About importing resource associations”](#) on page 169.

Specified schedules Specify the schedules that are used to import resources. You can specify schedules for full and update data imports.

 See [“Scheduling resource import rules”](#) on page 173.

- 4 Check the appropriate **Enabled** boxes to enable the importing of computer, user, subnet, and site resources.
- 5 Click **Apply**.

Scheduling resource import rules

For each resource import rule, you can specify the appropriate Full Import and Update Import schedules. A full import imports all resources from the targeted domain controller or domain.

An update import imports only the resources that have changed since the last time the resource import rule ran.

A single resource import rule may include both schedules, or you may configure different full import and update import rules. If you configure a specific update import rule, we recommend that the rule targets a domain controller rather than a domain.

An update import runs as a full import if any of the following are true:

- The rule is run for the first time.
- The domain or server that is specified in the rule has changed.
- The domain controller that the rule previously imported from is not available.

If necessary, you can override the schedule and run a resource import rule manually at any time.

See [“Creating and modifying resource import rules”](#) on page 171.

See [“Running resource import rules manually”](#) on page 176.

This task is a step in the process for importing resources using Microsoft Active Directory Import.

See [“Importing resources using Microsoft Active Directory Import”](#) on page 170.

To schedule resource import rules

- 1 In the Symantec Management Console, on the **Actions** menu, click **Discover > Import Microsoft Active Directory**.
- 2 On the **Microsoft Active Directory Import** page, beside the resource import rule that you want to schedule, check **Enabled**.
- 3 In the resource import rule description, click **Specified schedules**.
- 4 In the **Rule Scheduling** window, set up either or both of the following schedules:

Full Import Schedule	Imports all of the resources that the resource import rule identifies.
Update Schedule	Imports only the new and modified resources that the resource import rule identifies.

See [“To set up a schedule”](#) on page 175.

- 5 Click **OK** to close the **Rule Scheduling** page.
- 6 Click **Apply**.

To set up a schedule

- 1 Under the appropriate schedule, check **Enable**.
- 2 In the **Schedule** drop-down list, select one of the following schedules:

At date/time	Specify the appropriate date and time. If you want the schedule to repeat, check Repeat every , and then specify the repeat interval.
Shared schedule	Select the appropriate shared schedule.

Configuring the Directory Synchronization schedule

To keep the CMDB synchronized with Active Directory resources, you need to configure the appropriate Directory Synchronization schedule. The Directory Synchronization schedule identifies any previously imported resources that no longer exist in Active Directory and removes them from the CMDB. It also detects any resources that have been renamed or moved outside of the organizational units from which they were initially imported, and deletes the corresponding records from the CMDB.

Warning: If you move a computer from a domain to a workgroup, you must delete the computer's record from Active Directory to avoid duplication in the CMDB.

This task is a step in the process for importing resources using Microsoft Active Directory Import.

See [“Importing resources using Microsoft Active Directory Import”](#) on page 170.

To configure the Directory Synchronization schedule

- 1 In the Symantec Management Console, on the **Actions** menu, click **Discover > Import Microsoft Active Directory**.
- 2 In the **Microsoft Active Directory Import** page, under **Directory Synchronization Schedule**, check **Enabled**.

- 3 In the **Schedule** drop-down list, select one of the following schedules:

At date/time	Specify the appropriate date and time. If you want the schedule to repeat, check Repeat every , and then specify the repeat interval.
Shared schedule	Select the appropriate shared schedule.

- 4 Click **Apply**.

Running resource import rules manually

If you need to import particular resources immediately, you can run the appropriate resource import rule manually. You can run the resource import rule as a full import or an update import. Running a resource import rule manually has no effect on its schedule, if one is enabled.

See [“Scheduling resource import rules”](#) on page 173.

This task is a step in the process for importing resources using Microsoft Active Directory Import.

See [“Importing resources using Microsoft Active Directory Import”](#) on page 170.

To run resource import rules manually

- 1 In the Symantec Management Console, on the **Actions** menu, click **Discover > Import Microsoft Active Directory**.
- 2 In the **Microsoft Active Directory Import** page, select the resource import rule that you want to run.
- 3 Click one of the following options:

Run the selected import rule now (Full Import)	Runs a full import of the selected resource import rule.
Run the selected import rule now (Update Import)	Runs an update import of the selected resource import rule.

- 4 If you want to stop the import process for any reason, click **Stop**.

Discovering network devices

This chapter includes the following topics:

- [About Network Discovery](#)
- [Discovering network devices](#)
- [Delegating Network Discovery tasks to non-administrator users](#)
- [Importing MIB files](#)

About Network Discovery

Network Discovery lets you discover all IP devices that are connected to your network. Network Discovery lets you find new network devices and find the network devices whose discovery properties have changed.

Network Discovery is included in Symantec Management Platform.

Network Discovery can discover routers, switches, hubs, network printers, Novell NetWare servers, and the computers that are running Windows, UNIX, Linux, and Macintosh. You can use a variety of protocols to discover devices, such as AMT, SNMP, WMI, and others.

The information that is collected can help you do the following:

- Plan for imaging
- Updating drivers on specific types of hardware
- Configuring changes to routers or switches
- Identifying the computers that are running the operating systems not currently supported by the Symantec Management Agent

You can also update categories so that the new devices that are added to the network can be identified during discovery.

Because Network Discovery integrates with Symantec Management Platform, when devices are discovered, they are automatically created as resources in the platform’s central database (CMDB). Using the platform’s task management component, you can schedule discovery tasks to run when it best meets your needs.

See [“Discovering network devices”](#) on page 178.

See [“Delegating Network Discovery tasks to non-administrator users”](#) on page 188.

You can also discover Windows-based computers through domains or importing through Microsoft Active Directory.

See [“Resource discovery methods”](#) on page 162.

Discovering network devices

To help you successfully manage your network, you need to identify the various devices on your network. Network Discovery lets you find new network devices, identify previously-discovered network devices that are no longer found, and find network devices whose discovery properties have changed. The discovery is performed by running tasks that discover devices and reporting the data to the Notification Server. The discovery data about devices is stored as known resources in the Configuration Management Database (CMDB). To keep your discovery data current, you configure automated discovery tasks to run at regular intervals.

You can discover all the devices on your network and enter those devices in the CMDB.

See [“About Network Discovery”](#) on page 177.

Table 15-1 Process for discovering network devices

Step	Action	Description
Step 1	(Optional) Configure Network Discovery options.	You can configure default task options and configure SNMP classifications. See “Configuring discovery settings” on page 179.
Step 2	Create a Network Discovery task.	You can create and schedule a task to discover either a single device or multiple devices on a network. You can use two methods for creating tasks: using the Network Discovery wizard or creating tasks manually. See “Creating Network Discovery tasks using the wizard” on page 180. See “Manually creating and modifying Network Discovery tasks” on page 181.

Table 15-1 Process for discovering network devices (*continued*)

Step	Action	Description
Step 3	(Optional) Modify task settings or schedules.	After you create a Network Discovery task, you can modify the task settings or add additional schedules. See “Manually creating and modifying Network Discovery tasks” on page 181.
Step 4	View discovery data.	You can view the status of Network Discovery tasks and view reports that show discovery results. See “Viewing discovered devices in organizational views” on page 186. See “Viewing discovery reports” on page 187.
Step 5	Classify unknown devices.	If you have devices with an unknown classification, you can modify the SNMP classifications list. See “Classifying SNMP devices ” on page 187.

Configuring discovery settings

You can configure global settings for Network Discovery tasks. These settings are used when a new task is created.

You can configure Network Discovery in the following ways:

Discovery task settings

In the Network Discovery settings, you can set the maximum number of threads per discovery task. During the discovery process, a separate thread is used to discover each device.

This number is the default maximum thread count to use when a new Network Discovery task is created. You can also configure this count for an individual task by editing the advanced properties of the task.

You may want to reduce this value if discovery tasks place a burden on the server’s performance.

SNMP Device Classification

When you discover SNMP devices, you can identify a network device type classification with the resource. This method lets you identify resources as routers, switches, printers, servers, and so on. You can configure the classifications of discovered SNMP resources.

See [“Classifying SNMP devices ”](#) on page 187.

This task is a step in the process for discovering network devices.

See [“Discovering network devices”](#) on page 178.

To configure discovery settings

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Settings > Discovery and Inventory**, and then click **Network Discovery Settings**.
- 3 On the **Network Discovery Settings** page, enter the maximum number of threads per delivery task.

During the discovery process, a separate thread is used to discover each device.

This number is the default maximum thread count to use when a new Network Discovery task is created. You can also configure this count for an individual task by editing the advanced properties of the task.

You may want to reduce this value if discovery tasks place a burden on the server's performance.

- 4 Click **Save changes**.

Creating Network Discovery tasks using the wizard

The Network Discovery wizard is an administrator tool that guides you through creating a discovery task and configuring settings. You can later edit the task's advanced settings and schedules by editing the task.

This task is a step in the process for discovering network devices.

See [“Discovering network devices”](#) on page 178.

To create Network Discovery tasks using the Network Discovery wizard

- 1 In the Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Network Discovery**.
- 2 In the **Network Discovery Quick Start Actions** Web part, click **Launch Discovery Wizard**.
- 3 In the wizard, select a discovery method, and then click **Next**.
See [“Methods for discovering network devices”](#) on page 184.
- 4 Specify the portions of the network to discover, and then click **Next**.
See [“About selecting network ranges to discover”](#) on page 185.
- 5 Select a connection profile, and then click **Next**.

Connection profiles specify the protocols that you want to use for discovery. You can use an existing profile or create a new profile.

See [“Creating connection profiles with Network Discovery”](#) on page 182.

See [“Creating or cloning a connection profile”](#) on page 183.

- 6 Name the task and then click **Next**.
- 7 Schedule the task, and then click **Finish**.
See [“Adding a schedule to a policy, task, or job”](#) on page 354.
- 8 To view the tasks that the discovery wizard creates, view the bottom of the **Network Discovery Home** page.
You may need to click the refresh icon to view newly created tasks.

Manually creating and modifying Network Discovery tasks

You can manually create and modify tasks from the Task Management Portal. This option lets you configure advanced options and schedules. When you manually create tasks, you can discover a network or an individual device.

This task is a step in the process for discovering network devices.

See [“Discovering network devices”](#) on page 178.

To manually create a task to discover a network

- 1 In the Symantec Management Console, do one of the following:
 - On the **Home** menu, click **Discovery and Inventory > Network Discovery** and then in the **Network Discovery Task Management** Web part, on the **Available Tasks** tab, click **New**.
 - On the **Manage** menu, click **Jobs and Tasks**. In the left pane, expand **System Jobs and Tasks**, right-click **Discovery and Inventory**, and then click **New > Task**. In the **Create New Task** dialog box, in the left pane, under **Discovery and Inventory**, click **Discover Network**.
- 2 Give the task a unique and a descriptive name.
- 3 Select a connection profile.
Connection profiles specify the protocols that you want to use for discovery. You can use an existing profile or create a new profile .
See [“Creating connection profiles with Network Discovery”](#) on page 182.
See [“Creating or cloning a connection profile”](#) on page 183.
- 4 Select a discovery method.
See [“Methods for discovering network devices”](#) on page 184.
- 5 Specify the portions of the network to discover.
See [“About selecting network ranges to discover”](#) on page 185.
- 6 (Optional) To configure the maximum number of devices to discover concurrently, click **Advanced**.

- 7 Click **OK**.
- 8 In the task window that opens, schedule the task.
See [“Adding a schedule to a policy, task, or job”](#) on page 354.
- 9 To view the task, in the left pane, click **Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory**. You may need to click the refresh icon to view newly created tasks.

To manually create a task to discover a single device

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**. In the left pane, expand **System Jobs and Tasks**, right-click **Discovery and Inventory**, and then click **New > Task**.
- 2 In the **Create New Task** dialog box, in the left pane, under **Discovery and Inventory**, click **Discover Device**.
- 3 Give the task a unique and a descriptive name.
- 4 Select a connection profile.
Connection profiles specify the protocols that you want to use for discovery. You can use an existing profile or create a new profile.
See [“Creating connection profiles with Network Discovery”](#) on page 182.
See [“Creating or cloning a connection profile”](#) on page 183.
- 5 Click **OK** to save the task.
- 6 In the task window that opens, click **New Schedule**.
- 7 In the **New Schedule** dialog box, schedule the task, specify the device that you want to discover by entering the IP address or name, and then click **Schedule**.
See [“Adding a schedule to a policy, task, or job”](#) on page 354.
- 8 To view the task, in the left pane, click **Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory**. You may need to click the refresh icon to view newly created tasks.

Creating connection profiles with Network Discovery

Network Discovery tasks use connection profiles to configure the protocols that are used to communicate with network devices. Connection profiles are a component of the Symantec Management Platform. How you use protocols and connection profiles has important ramifications on how Network Discovery is able to discover devices.

Network Discovery uses connection profiles to connect to the target devices using the enabled protocols in the profile. When a device is discovered, a resource for that device is created in

the CMDB. The resource keeps a record of the protocols that were used to communicate with the device.

If changes are made in the connection profiles regarding the protocols used or the credentials used for those protocols, and if you want to discover devices using those changed settings, you need to run a discovery again.

You can create and use different connection profiles depending on the type of devices and the protocols that are used in your network. When configuring Network Discovery tasks, you can use an existing connection profile or create your own.

See [“Creating Network Discovery tasks using the wizard”](#) on page 180.

See [“Manually creating and modifying Network Discovery tasks”](#) on page 181.

To create a connection profile

- 1 In a Network Discovery task, click **New** connection profile.
The listed protocols are those that are supported.
- 2 Name the connection profile.
- 3 Turn on or off each protocol and configure the operational settings and select credentials for each protocol.
See [“Managing credentials”](#) on page 88.
- 4 Click **OK**.
- 5 Select the profile from the drop-down list.

Creating or cloning a connection profile

Connection profiles store the information that is required to communicate with computers and other network devices using standard network monitoring protocols. These protocols include SNMP, WMI, WSMAN, and several others.

Connection profiles are associated with devices during network discovery. During discovery, a connection profile is selected to define the protocols and credentials to use. When discovery completes, this connection profile is then associated with each discovered resource. When information is required, the associated connection profile is used to connect.

Typically, you should create a new connection profile for each segment of your network that uses different network monitoring credentials.

To create a connection profile

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Monitoring and Alerting > Protocol Management > Connection Profiles**, and then click **Manage Connection Profiles**.

- 3 On the **Manage Connection Profiles** page, click **Add settings**, and provide a name for the new profile.
- 4 In the **Define Group Settings** dialog box, type the name of the new profile, enable the protocols that you want, and provide the required protocol details.

 At the upper right next to each protocol that you want to enable, click the colored circle, and then click **On**.

 For more information, click the page and then press **F1**.
- 5 Click **OK**.

Methods for discovering network devices

When discovering network devices, you can use one of the following discovery methods: ping or ARP.

See [“Discovering network devices”](#) on page 178.

You launch discovery tasks through the Network Discovery wizard, which you access from the Network Discovery home page. This is where you indicate which method of discovery you want to use.

See [“Creating Network Discovery tasks using the wizard”](#) on page 180.

See [“Manually creating and modifying Network Discovery tasks”](#) on page 181.

Table 15-2 Network discovery methods

Method	Description
Ping	<p>Device existence is determined by sending an ICMP ping request to each possible IP address in a specified range or subnet. When a device receives a ping, it responds with a reply, reporting the presence of the device to the discovery engine.</p> <p>You can use this method to perform a comprehensive search that finds all devices.</p> <p>This method is unusable if your network firewall does not allow Ping requests.</p> <p>This method may not be best for the subnets that are sparse (those with few devices in their address space). The engine may spend a lot of time waiting for responses from the devices that don't exist. This situation occurs because the engine waits until the specified timeout period expires, and then, if applicable, the engine retries one or more times.</p>

Table 15-2 Network discovery methods (*continued*)

Method	Description
ARP	<p>Device existence is initially determined by reading the ARP Cache table of a network infrastructure device (such as a switch or router). The ARP Cache table is read from the device, and then each device in the table is individually contacted and discovered.</p> <p>This discovery method gives the discovery engine a set of devices to discover.</p> <p>However, ARP Cache table entries are removed after relatively short periods of inactivity. This means that the scan by itself is not aware of inactive devices. You can fix this issue by sending a ping to each device in a target network. This process refreshes the table, which has all of the devices in it.</p>

About selecting network ranges to discover

When you create a Network Discovery task, you identify either the single network device or ranges of addresses that you want to discover. You do this by specifying the addresses that you either want to include or exclude or a combination of both.

See [“Creating Network Discovery tasks using the wizard”](#) on page 180.

See [“Manually creating and modifying Network Discovery tasks”](#) on page 181.

If you have a seed device and then create an include range, the seed device must be included within the include range to also be discovered.

To use a custom range, you can use wildcards or ranges of values in the third or fourth octet of the address. The following are examples of how you can use a custom range:

172.16.[*].[*]	You can use an asterisk as a wildcard that equals any value from 0-254.
172.16.[1-24].[1-254]	You can specify a range of values. Any address in the range is included or excluded.
172.16.[3-30].[1-10]	

You can also import a text file to specify the addresses that you want to include or exclude. When you configure a text file, you must include all the information required for that type of address or range. For example, if you specify an IP range, you must include the starting IP address, the ending IP address, and the mask. You can also specify custom IP ranges in an import file.

The following is an example of the format of an import file:

```
SingleIpAddr, Include, 192.168.0.2,
```

```
SingleIpAddr, Exclude, 192.168.0.3,

Hostname, Include, hostname1.company1.com
Hostname, Exclude, hostname2

Subnet, Include, 192.168.0.0, 255.255.255.0
Subnet, Exclude, 192.169.0.0, 255.255.255.0

CustomIpAddrRange, Include, 192.168.*.*, 255.255.0.0
CustomIpAddrRange, Exclude, 10.192.1-25.1-254, 255.0.0.0
CustomIpAddrRange, Include, 10.192.4.1-100, 255.255.254.0

IpAddrRange, Include, 192.168.0.1, 192.168.0.200, 255.255.255.0
IpAddrRange, Exclude, 192.168.0.120, 192.168.1.140, 255.255.255.0
```

Viewing discovered devices in organizational views

When a device is discovered, a resource for that device is automatically created for it in the Configuration Management Database (CMDB). You can view the devices using organizational views. Organizational views display all the known resources in your environment. You can view all discovered devices in one view, called Network Resources. There are also views for individual resource types, such as computer, network printer, and so on.

If the resource type of the device is known, the resource type is displayed as a property of the resource. If a device has a resource type of 'Network Resource', then the device type is unknown. These unknown devices are listed in the Network Resource view, not in any of the specific resource type views. If you have the devices that have an unknown classification, you can modify the SNMP classification list.

See [“Classifying SNMP devices”](#) on page 187.

This task is a step in the process for discovering network devices.

See [“Discovering network devices”](#) on page 178.

To view discovered devices in organizational views

- 1 In the Symantec Management Console, on the **Manage** menu, click **All Resources**.
- 2 In the left pane, expand **Default > All Resources > Asset**, and then click **Network Resource**.

To view a specific type of resource, in the left pane, click a resource type under **Network Resource**.

- 3 (Optional) To export the list of discovered devices into a spreadsheet or HTML file, do the following:

- On the toolbar, click **Save As**, and then click the file format into which you want to export the data.
- In the **Save As** dialog box, select if you want to export all resources, selected resources, or the resources that you filtered using the **Search** box, and then click **OK**.
- In the **Save As** dialog box, select the folder in which to save the file, and then click **Save**.

Viewing discovery reports

You can view the results of your discovery through reports. You can view predefined reports or create your own.

The Discovered Devices report lets you filter the results that are based on a date range, the discovery method or protocol used, or the task that was used.

The Discovered Devices by Group report lets you group the results that are based on a date range, the discovery method or protocol used, the task that was used, or the device type.

This task is a step in the process for discovering network devices.

See [“Discovering network devices”](#) on page 178.

To view discovery reports

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, expand **Reports > Discovery and Inventory**, and then click the report that you want to view.
- 3 Enter the parameters of the report, and click **Refresh**.

See [“About Notification Server reports”](#) on page 367.

Classifying SNMP devices

Discovered SNMP devices are identified by their device type, such as computer, network printer, and so on. For the device type to be identified, Network Discovery must know the SNMP device classification about that type. Network Discovery has a predefined list of common SNMP devices. If the device that is discovered is in that list, then it can be identified. If the device is not in the list, it is identified with the generic resource type **Network Resource**.

You can view the predefined list on the **Device Classifications** page. This page lists classifications of commonly used devices. This data includes the SNMP object ID, device type, manufacturer, and device model. If the SNMP object ID that is discovered matches an item from this list, the data is populated.

Before you run a Network Discovery task, you can review the device classification list, which contains common manufacturers. If you find the list incomplete, you can add or edit classifications to customize this list for your network environment. Taking time to review and

customize the device classification list results in more complete discovery data. Doing this task before a discovery is not required. You can do this task after a discovery, but you have to re-run the discovery to get the updated classification.

If you change the information for an existing SNMP device classification, you need to rescan any device that was previously classified using that entry. Rescanning is necessary so that the devices with changed information are reclassified.

After you run a Network Discovery task, you may have devices with an unknown classification. If you know the Object ID for these devices, you can add them to the classification list. The next time you run a Network Discovery task, the devices will use the updated list to be classified.

You can configure the SNMP device classification values that are used to identify SNMP devices. A list of common devices is provided in Network Discovery. You can add, edit, or remove classifications to customize this list for your network environment. After you change a device classification, you must rediscover it so that it can be reclassified.

This task is a step in the process for discovering network devices.

See [“Discovering network devices”](#) on page 178.

To classify SNMP devices

- 1 In the Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Network Discovery**.
- 2 In the **Network Discovery Quick Start Actions** Web part, click **SNMP Device Classification**.
- 3 To add a new classification, click **Add**, and enter the information about your device.
The SNMP object ID must be a unique value that you can obtain from the device manufacturer.
- 4 You can also edit or remove classifications to match the devices in your network environment.
- 5 To re-classify the devices that are based on new settings, you must re-run the discovery.

Delegating Network Discovery tasks to non-administrator users

As a network administrator, you may have a team of other administrators to whom you can delegate certain network-administration tasks. Whether you work alone or with a team of administrators, you may need to delegate Network Discovery tasks to other, non-administrator users.

Network Discovery tasks require rights to work with connection profiles and credentials. These rights are granted through a combination of permissions and privileges. Permissions are

assigned by default to items, such as files, tasks, and wizards. Privileges are granted to user roles, including the predefined administrator role and the predefined non-administrator roles. The intersection of the item permissions and role privileges determines what administrators and non-administrators can do to items.

See [“About Network Discovery”](#) on page 177.

Each of the predefined non-administrator roles in Symantec Management Platform includes inherent privileges.

See [“Predefined security roles”](#) on page 80.

See [“Security privilege categories”](#) on page 418.

To enable users to discover network devices and work with connection profiles and credentials, you assign privileges to the user roles that enable those roles to create connection profiles and credentials. Then, you select a non-administrator user role to which you assign users. You then limit or augment the scope of the role by removing or assigning specific privileges. To create and run Network Discovery tasks, the user role must have access to at least one default connection profile. This profile can be the default connection profile.

The Symantec Supervisors role is a higher-level non-administrator role. Other workers can be assigned a role with limited inherent rights. The Symantec Level 1 Workers and Symantec Level 2 Workers roles are good examples. These roles are used in some of the tasks that are included in the process that is defined in this topic. You are not limited to these roles. They are the predefined roles that are the most useful to administrators.

You can delegate tasks to more than one user role. To create, edit, or run tasks, a user must be a member of a security role that has the Discovery Task Management privilege.

The default Symantec Supervisors role includes more access to Network Discovery than other non-administrator roles. Delegating tasks to the Symantec Supervisors role is less complicated than delegating tasks to roles that have no access to perform any Network Discovery tasks.

Select a role to which to delegate tasks based on what you want non-administrators to be able to do. Delegate tasks by completing each step in the process, in order. Tasks that are listed in later steps may depend on the rights that are granted in preceding steps.

Table 15-3 Process for delegating Network Discovery tasks to non-administrator users

Step	Task	Description
Step 1	Add non-administrators to security roles for performing Network Discovery tasks.	To delegate tasks to users in non-administrator roles, you must assign users to those roles. See “Adding non-administrator users to security roles for performing Network Discovery tasks” on page 191.

Delegating Network Discovery tasks to non-administrator users

Table 15-3 Process for delegating Network Discovery tasks to non-administrator users
(continued)

Step	Task	Description
Step 2	Enable non-administrator roles to create or run Network Discovery tasks.	<p>You can delegate Network Discovery tasks to non-administrator roles and assign non-administrator users to those roles. Several default roles are included in Symantec Management Platform, and each has certain inherent rights.</p> <p>The Symantec Supervisors role can run Network Discovery tasks. Other non-administrator roles cannot even run existing tasks until you grant the required privilege to the role. You must perform certain steps to enable non-administrator roles to create and run Network Discovery tasks.</p> <p>By default Administrators, Symantec Supervisors, and Symantec Level 1 and Level 2 Workers can view the Network Discovery portal page. This page is a convenient location from which administrators view and run Network Discovery tasks. Administrators and supervisors can view all parts of this page by default. However, the Network Discovery Task Management Web part is disabled for other users. To let other non-administrator users view and use this Web part, assign them to a security role that has the Discovery Task Management privilege enabled.</p> <p>See “Predefined security roles” on page 80.</p> <p>See “Enabling non-administrator roles to create or run Network Discovery tasks” on page 192.</p>
Step 3	(Optional but recommended) Grant non-administrator roles privileges to create credentials and connection profiles.	<p>A non-administrator role can be given privileges to discover network devices and to create or edit credentials and connection profiles. Creating or editing credentials and connection profiles may be necessary for performing the tasks that are listed later in this process.</p> <p>This step is optional because users can create Network Discovery tasks without these privileges. They would simply have to use existing connection profiles to which they have access.</p> <p>See “Security privilege categories” on page 418.</p> <p>See “Granting non-administrator roles privileges to create credentials and connection profiles” on page 195.</p>
Step 4	Grant non-administrator roles access to the default connection profile.	<p>To create and run Network Discovery tasks, a user role must have access to the default connection profile (or other connection profile, but at least one).</p> <p>See “Granting non-administrator roles access to the default connection profile” on page 196.</p>

Table 15-3 Process for delegating Network Discovery tasks to non-administrator users
(continued)

Step	Task	Description
Step 5	Enable roles other than predefined security roles to create and run tasks using the Network Discovery wizard.	<p>The following security roles are predefined and by default can create and run tasks using the Network Discovery wizard:</p> <ul style="list-style-type: none"> ■ Administrator ■ Symantec Supervisors ■ Symantec Level 2 Workers ■ Symantec Level 1 Workers <p>If you need to let other roles create and run tasks using the wizard, you must give them access explicitly.</p> <p>See “Enabling roles other than predefined security roles to create and run tasks using the Network Discovery wizard” on page 196.</p>
Step 6	(Optional) Make a connection profile read-only.	<p>If you want to let a particular non-administrator role view but not edit a connection profile, then you can make the profile read-only.</p> <p>See “Making a connection profile read-only” on page 198.</p>

Adding non-administrator users to security roles for performing Network Discovery tasks

If you want to delegate Network Discovery tasks to non-administrator users, they must have the privileges necessary to perform those tasks. Privileges are assigned to user roles. If you have not created a Windows user to perform Network Discovery tasks, you must create this user first. Then, add the user to your chosen security role or create a custom role. Finally, grant privileges to the security role. You can then delegate the tasks that the role has sufficient privileges to perform.

The Network Discovery portal page is a convenient location from which to view and perform discovery tasks. Administrators and Symantec Supervisors have full access to this page by default. Users in other, non-administrator roles can view this page. However, the **Discovery Task Management** Web part is disabled unless you enable it with the Discovery Task Management privilege. By adding non-administrators to security roles and granting rights for Network Discovery task management, you enable them to view and work from this page.

See [“Enabling non-administrator roles to create or run Network Discovery tasks”](#) on page 192.

Symantec Management Platform includes several non-administrator, predefined security roles by default. You can also create custom security roles.

See [“Predefined security roles”](#) on page 80.

See [“Creating and configuring Symantec Management Platform user accounts”](#) on page 191.

This task is a step in the process for delegating Network Discovery tasks to non-administrators.

See [“Delegating Network Discovery tasks to non-administrator users”](#) on page 188.

To add non-administrator users to security roles for performing Network Discovery tasks

- 1 Log on to Symantec Management Console as Administrator.
- 2 To create a new Windows user, do the following:
 - In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
 - In the left pane, click **Accounts**.
 - On the **Accounts** page, click **Add**.
 - In the **New Account** dialog box, enter a name for the new user and click **OK**.
 - In the right pane, on the **General** tab, under **Account details**, in the **Full Name** field, enter the user's full name.
You can leave the **Email** field empty. It is not required for this procedure.
 - Under **Credentials**, click **Add Credential > Windows**.
 - In the **Windows Credential** dialog box, enter the logon name that corresponds with the Windows user who is associated with this new account and click **OK**.
 - Enable the account.
At the upper right of the page, click the colored circle, and then click **On**.
- 3 To add the user to a security role to which you want to delegate tasks, do the following:
 - On the **Member Of** tab, click **Add Role**.
 - In the **Select Role(s)** dialog box, click **Symantec Level 1 Workers** or other role to which you want to assign this user, and then click **OK**.
If none of the predefined security roles meets your needs, you can create a custom security role.
See [“Creating and configuring security roles”](#) on page 65.
- 4 Click **Save changes**.

Enabling non-administrator roles to create or run Network Discovery tasks

You can delegate Network Discovery tasks to users outside the Symantec Administrators group. To delegate tasks, you assign privileges to non-administrator roles. You then add users to those non-administrator roles.

This topic describes how to delegate common Network Discovery tasks to the following non-administrator roles:

- Symantec Supervisors.
 By default, users in this role can run existing Network Discovery tasks. However, they cannot create tasks by default. This is because they do not have access to the default connection profile unless you grant that access explicitly.
- Symantec Level 1 and Level 2 Workers.
 Users in these roles have limited rights. They cannot even run existing tasks until you give them rights to do so.

You are not limited to using these non-administrator roles. They are shown in this topic as examples. Use whichever predefined security role serves your purpose.

See [“Predefined security roles”](#) on page 80.

Tasks use connection profiles, which use credentials. For any non-administrator role to create new tasks (and not merely run them), you must set access permissions to a connection profile. You then set a level of control (the maximum level is **Full Control**) to protocol settings for that role. After you set these permissions, users in a non-administrator role can perform the tasks that you specify.

To enable non-administrators to create Network Discovery tasks, you must complete the following procedures:

- Grant rights to a non-administrator role for network discovery task management. This procedure lets users in the role run tasks.
- Add the role of your choice to the access permissions of the relevant connection profile. Then allow this role control to protocol settings. After you add the role to a connection profile, users in that role can create and edit Network Discovery tasks.

This task is a step in the process for delegating Network Discovery tasks to non-administrators.

See [“Delegating Network Discovery tasks to non-administrator users”](#) on page 188.

To grant rights to a non-administrator role for network discovery task management

- 1 Log on to Symantec Management Platform as Administrator.
- 2 In the Symantec Management Console on the **Settings** menu, click **Security > Account Management**.
- 3 In the left pane, under **Account Management**, click **Roles**.
- 4 On the **Roles** page, in the left pane, click the non-administrator role to which you want to delegate creating and running Network Discovery tasks.

Typical roles to which administrators delegate these tasks are Symantec Level 1 Workers and Symantec Level 2 Workers.

- 5 On the right, in the window that is labeled with the role that you selected, click the **Privileges** tab if it is not active.
- 6 Under **Management Privileges**, check **Discovery Task Management**.

- 7 If the role that you have selected also needs to create or edit connection profiles, check the following additional options:
 - Under **Connection Profile Privileges**, check **Create Connection Profile**.
 - Under **System Privileges**, check **View Security**.
 - Under **Credential Privileges**, check **Create Credential**.

8 Click the **Members** tab.

9 Ensure that the user you want to add to the selected role has been added to this role.

If the user is not a member of this role, you must create a Notification Server user and add the user to the relevant role.

See [“Adding non-administrator users to security roles for performing Network Discovery tasks”](#) on page 191.

10 Click **Save changes**.

To grant a predefined role full (or lesser) control to protocol settings

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, under **Settings**, expand **Monitoring and Alerting > Protocol Management > Connection Profiles**, and then click **Manage Connection Profiles**.
- 3 On the **Manage Connection Profiles** page, click **Default Connection Profile**, and then click **Edit**.
- 4 In the **Define Group Settings** dialog box, click **Access permissions to protocols settings**.
- 5 Click **Add**, select the role to which you want to grant control, and click **Select**.

Symantec Level 1 Workers Users in this role have fewer rights than Symantec Supervisors by default. When given Discovery Task Management privileges and Full Control, these workers can create and run Network Discovery tasks.

Symantec Level 2 Workers Users in this role have fewer rights by default. When given Discovery Task Management privileges and Full Control, these workers can create and run Network Discovery tasks.

Symantec Supervisors Users in this role can run Network Discovery tasks by default. When given Full Control, these workers can also create and edit Network Discovery tasks.

6 In the **Permission Selection** dialog box, select permissions in one of the following ways:

- Check **Use** and **Read**. You can check any other boxes that correspond to the tasks that you want the selected role to be able to perform. Then click **Select**.
 - Click **Full Control** to give the role all available rights that are listed, and then click **Select**.
- 7 In the **Security Descriptor Settings for: Default Connection Profile** dialog box, click **Apply**.
 - 8 In the **Define Group Settings** dialog box, click **OK** to save the connection profile.

Granting non-administrator roles privileges to create credentials and connection profiles

When you delegate tasks to non-administrator roles, you must determine which tasks the users who are assigned to those roles can perform. Each Symantec Management Platform predefined security role includes inherent rights.

See [“Predefined security roles”](#) on page 80.

One example is the default Symantec Supervisors role. Users who are assigned to this role can run existing tasks without the role being granted additional privileges. These users can also create Network Discovery tasks if they have access to an existing connection profile.

However, to let non-administrator roles create new tasks and connection profiles, you grant privileges to those roles to create credentials and connection profiles. These additional privileges are necessary if users are expected to create new tasks that may require some credentials and connection profiles that are different from the existing credentials and profiles.

See [“Configuring discovery settings”](#) on page 179.

To let users assigned to non-administrator roles create credentials and connection profiles, you must enable those privileges for the role. These privileges let the users create the credentials and the connection profiles that are suited to the tasks that you delegate to them or that they create.

This task is a step in the process for delegating Network Discovery tasks to non-administrators.

See [“Delegating Network Discovery tasks to non-administrator users”](#) on page 188.

To grant non-administrator roles privileges to create credentials and connection profiles

- 1 Log on to the Symantec Management Console as Administrator.
- 2 In the Symantec Management Console, on the **Settings** menu, click **Security > Account Management**.
- 3 Under **Account Management**, click **Roles**
- 4 On the **Roles** page, click the role that you want to enable, and in the right pane, click the **Privileges** tab.

- 5 Scroll to **Connection Profile Privileges** and check **Create Connection Profile**.
- 6 Scroll to **Credential Privileges** and check **Create Credential**.
- 7 Scroll to **System Privileges** and check **View Security**.
- 8 Click **Save changes**.

Granting non-administrator roles access to the default connection profile

Users in non-administrator roles, need access to the default connection profile to run tasks. After you grant these roles access to the default connection profile, users in those roles can also create tasks. They cannot create connection profiles, but they can create tasks that use existing connection profiles.

This task is a step in the process for delegating Network Discovery tasks to non-administrators. See [“Delegating Network Discovery tasks to non-administrator users”](#) on page 188.

To grant a predefined role full (or lesser) control to the default connection profile

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, under **Settings**, expand **Monitoring and Alerting > Protocol Management > Connection Profiles** and click **Manage Connection Profiles**.
- 3 On the **Manage Connection Profiles** page, click **Default Connection Profile**, and then click **Edit**.
- 4 In the **Define Group Settings** dialog box, click **Access permissions to protocols settings**.

Enabling roles other than predefined security roles to create and run tasks using the Network Discovery wizard

The Network Discovery wizard is an administrator tool bundled with Symantec Management Platform. It is one method for discovering network devices and performing other discovery tasks.

You access the Network Discovery wizard from the Symantec Management Console **Home** menu.

See [“Creating Network Discovery tasks using the wizard”](#) on page 180.

The following security roles are predefined and by default can create and run tasks using the Network Discovery wizard:

- Administrator
- Symantec Supervisors

- Symantec Level 2 Workers
- Symantec Level 1 Workers

You may want to enable other roles to create and run tasks from the Network Discovery wizard. In this case, you must give those roles the privileges that are required to perform those tasks using the wizard.

This task is a step in the process for delegating Network Discovery tasks to non-administrators.

See [“Delegating Network Discovery tasks to non-administrator users”](#) on page 188.

To enable roles other than predefined security roles to create tasks using the Network Discovery wizard

- 1 Log on to Symantec Management Platform as Administrator.
- 2 In the Symantec Management Console, on the **Settings** menu, click **Security > Permissions**.
- 3 In the **Security Role Manager**, in the **Role** drop-down box, select the role that you want to enable to run tasks.
- 4 In the **View** drop-down list, click **Settings**.
- 5 In the left pane, click **Edit**.

Note that in the **Items Selector** dialog box, if the **Settings** checkbox is checked, all other options are grayed out.

- 6 If **Settings** is checked, uncheck it.
- 7 Under **Discovery and Inventory**, check **Network Discovery Wizard** if it is not checked already.
- 8 Re-check **Settings** to turn on inheritance again.
- 9 Click **Save Changes**.

To enable roles other than predefined security roles to schedule and run tasks using the Network Discovery wizard

- 1 Log on to Symantec Management Platform as Administrator.
- 2 In the Symantec Management Console, on the **Settings** menu, click **Security > Permissions**.
- 3 In the **Security Role Manager**, in the **Role** drop-down box, click the role that you want to enable.
- 4 In the **View** drop-down box, click **Tasks**.

- 5 In the left pane, under **Tasks**, expand **Jobs and Tasks > System Jobs and Tasks** and click **Discovery and Inventory**.

Note that in the **Discovery and Inventory** pane, the **Inherited** section is gray and cannot be edited.
- 6 In the **Discovery and Inventory** pane, under **Noninherited**, scroll down to **Task Server Permissions**, and check **Run Task**.
- 7 Click **Save changes**, and close the **Security Role Manager**.

Making a connection profile read-only

You may need to delegate Network Discovery tasks to users in non-administrator roles. However, you may not want these users to change connection profiles. You would make a connection profile read-only to prevent hacking and maintain the security and privacy of confidential information. Another reason to make a connection profile read-only is to prevent less-experienced users from modifying a connection profile to use unsupported protocols.

If you want to limit users to viewing credentials and running Network Discovery tasks, you can block Write rights to each connection profile. By blocking Write rights from a non-administrator role, you make a connection profile Read-only to users in that role. The users who are assigned to those non-administrator roles whose Write rights you block can still view and run tasks, but they cannot change that connection profile or create a connection profile.

This task is a step in the process for delegating Network Discovery tasks to non-administrators. See [“Delegating Network Discovery tasks to non-administrator users”](#) on page 188.

To make a connection profile read-only

- 1 Log on to the Symantec Management Console as Administrator.
- 2 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 3 In the left pane, under **Settings**, expand **Monitoring and Alerting > Protocol Management > Connection Profiles** and click **Manage Connection Profiles**.
- 4 In the **Manage Connection Profiles** pane, click **Default Connection Profile**, and then click **Edit**.
- 5 In the **Define Group Settings** dialog box, click **Access permissions to protocol settings**.
- 6 In the **Security Descriptor Settings for: Default Connection Profile** dialog box, select the role, such as **Symantec Level 2 Workers**, and click **Edit**.
- 7 In the **Permission Selection** dialog box, uncheck **Write**, and click **Select**.
- 8 In the **Security Descriptor Settings for: Default Connection Profile** dialog box, click **Apply** to save the settings, and in the **Define Group Settings** dialog box, click **OK** to save the connection profile.

Importing MIB files

You can use two methods to import MIB files into the database. You can manually import MIB files one at a time using the MIB Import utility. You can also create and schedule a task that imports one or more MIB files.

To import MIB files manually using the MIB Import utility

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Monitoring and Alerting > SNMP MIB Import Browser**, and then click **MIB Browser**.
- 3 On the **MIB Browser** page, click **Import MIB file**.
- 4 In the **Import Mib File** dialog box, click **Browse**, select the file, and then click **Import**.

You can import any additional MIB files that you require.

To import MIB files using the MIB Import task

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, right-click the folder where you want to create the task and click **New > Task**.
- 3 In the **Create New Task** dialog box, in the left pane, under **Monitoring and Alerting**, click **MIB Import**.

- 4 Rename the task, select the MIB file to upload, and specify the import option.

You can choose to either import the single MIB file, or you can choose to import additional MIB files that are stored at the directory location.

- 5 Click **Upload** to upload the MIB file into the import task.
- 6 If you want to import multiple MIB files, then continue to browse and upload each MIB file that you require into the task.
- 7 Click **OK**.
- 8 Select the new MIB import task.

By default, the new MIB import task is stored at: **System Jobs and Tasks > Notification Server**.

- 9 Schedule the new MIB import task to run by using the task scheduling utility.

See [“Adding a schedule to a policy, task, or job”](#) on page 354.

Installing and configuring the Symantec Management Agent

- [Chapter 16. Introducing the Symantec Management Agent](#)
- [Chapter 17. Installing the Symantec Management Agent on client computers](#)
- [Chapter 18. Upgrading and uninstalling the Symantec Management Agent](#)
- [Chapter 19. Configuring the Symantec Management Agent](#)

Introducing the Symantec Management Agent

This chapter includes the following topics:

- [About the Symantec Management Agent](#)
- [Opening the Symantec Management Agent user interface](#)
- [Enabling the Diagnostics mode in Symantec Management Agent](#)

About the Symantec Management Agent

The Symantec Management Agent is the software that establishes communication between the Notification Server computer and the computers in your network. Computers with the Symantec Management Agent installed on them are called managed computers. The Notification Server computer interacts with the Symantec Management Agent to monitor and manage each computer from the Symantec Management Console.

The Notification Server computer and the Symantec Management Agent work together to provide the following types of functionality for managed computers:

- Monitoring hardware and software
- Scheduling software installations and file updates
- Collecting basic inventory information
- Managing policies and packages

You can install the Symantec Management Agent on Windows, Linux, UNIX, and Mac computers. The Symantec Management Agent also lets you install and manage solution agent plug-ins that add additional functionality to the agent. For example, installing the Inventory plug-in lets you gather detailed hardware and software information from all of your managed computers.

See [“Methods for installing the Symantec Management Agent”](#) on page 204.

If you want to use Cloud-enabled Management, there is a special procedure for installing and setting up the Symantec Management Agent to work in this environment.

See [“About Cloud-enabled Management”](#) on page 252.

Opening the Symantec Management Agent user interface

You can open the Symantec Management Agent user interface in several ways.

See [“About the Symantec Management Agent”](#) on page 201.

To open the Symantec Management Agent user interface on a Windows computer, do one of the following:

- On the **Start** menu, click **Programs > Symantec > Symantec Management Agent**.
- In the notification area, double-click the Symantec Management Agent icon.
- In the notification area, right-click the Symantec Management Agent icon and then click **Symantec Management Agent**.
- Run the following command:

```
install path\Altiris\Altiris Agent\AeXAgentActivate.exe
```

To open the Symantec Management Agent user interface on a Mac computer, do the following:

- Open `Symantec Management Agent.app` application that is located at `/Applications/Utilities/.`

Enabling the Diagnostics mode in Symantec Management Agent

(Windows only)

The **Diagnostics** mode in Symantec Management Agent lets you view various statistical information about the client computer and work with the tools that help you troubleshoot the Symantec Management Agent. For example, you can check the network activity in real time and view the statistical information about the connections to Notification Server and site servers. You can also view the policies and schedules that apply to this computer and activate or deactivate the plug-ins that are installed.

Note that you must be logged in as an administrator to enable the Diagnostics mode in Symantec Management Agent.

See [“About the Symantec Management Agent”](#) on page 201.

To enable the Diagnostics mode in Symantec Management Agent

- 1 On the client computer, open a command prompt window as an administrator and go to the following directory:

```
install_path\Program Files\Altiris\Altiris Agent
```

- 2 Run the following command: `aexnsagent /diags`
- 3 On the Symantec Management Agent toolbar, click **View > Diagnostics**.

After you enable the Diagnostics mode, the **Diagnostics** option appears on the Symantec Management Agent toolbar and lets you open the tabs that you want.

Installing the Symantec Management Agent on client computers

This chapter includes the following topics:

- [Methods for installing the Symantec Management Agent](#)
- [Installing the Symantec Management Agent on Windows computers](#)
- [Installing the Symantec Management Agent on UNIX, Linux, and Mac computers](#)

Methods for installing the Symantec Management Agent

Before you install the Symantec Management Agent, Symantec recommends that you plan your installation using the *IT Management Suite Planning for Implementation Guide*.

You can install the Symantec Management Agent on Windows, UNIX, Linux, and Mac computer.

See [“About the Symantec Management Agent”](#) on page 201.

After the Symantec Management Agent gets installed on the client computer, the agent sends a registration request to Notification Server to establish trusted communication.

Table 17-1 Methods for installing the Symantec Management Agent

Method	Description
Manual push	<p>Pushing is initiated from the Symantec Management Console and installs the Symantec Management Agent immediately. You can install the Symantec Management Agent on any number of computers in the same push operation. You can also customize the installation options for each push operation.</p> <p>For UNIX, Linux, and Mac computers, this method requires that an SSH server is running. You must also configure the firewall to accept SSH connections on the target computers.</p> <p>See "Installing the Symantec Management Agent for Windows with a manual push" on page 211.</p> <p>See "Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual push" on page 223.</p> <p>The agents that you install with manual push bypass the agent registration process and the communication between the agent and Notification Server is automatically established.</p>
Manual pull	<p>Pulling is initiated from the computer on which the Symantec Management Agent is to be installed. This operation lets you work around firewalls and the network access limitations that may prevent push installations to remote computers. For UNIX, Linux, and Mac computers, you need to use this method if SSH is not available.</p> <p>See "Installing the Symantec Management Agent for Windows with a manual pull" on page 213.</p> <p>See "Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual pull" on page 226.</p>
Scheduled push	<p>This method is available for Windows computers only.</p> <p>A scheduled Symantec Management Agent installation is performed at a defined time, unlike the manual push installations which are performed immediately. You can push the Symantec Management Agent to the computers in an organizational group, filter, or resource target, or the computers that have selected resources.</p> <p>Note that the agents that you install with scheduled push do not bypass the agent registration process.</p> <p>See "Performing a scheduled installation of the Symantec Management Agent for Windows" on page 214.</p>

Table 17-1 Methods for installing the Symantec Management Agent (*continued*)

Method	Description
Agent upgrade policy	<p>The Symantec Management Agent Upgrade policy is provided with Symantec Management Platform. You can turn on this policy and configure it to ensure that all of your managed computers have the correct Symantec Management Agent version installed.</p> <p>See “Configuring the Symantec Management Agent Upgrade and Uninstall policies” on page 230.</p>
Install the Symantec Management Agent on the computers that cannot directly connect to the internal network.	<p>If you want to use Cloud-enabled Management, there is a special procedure for installing and setting up the Symantec Management Agent to work in this environment.</p> <p>See “About Cloud-enabled Management” on page 252.</p> <p>See “Generating and installing the Cloud-enabled Management offline package” on page 269.</p>

Note: When you install the Symantec Management Agent on a computer, there is a delay before the Client Task Agent registers with Notification Server. Any tasks that are targeted at the computer during this time (typically about 10 minutes) have a pending status until the Client Task Agent registers. When the Client Task Agent is registered, the tasks are executed immediately.

Installing the Symantec Management Agent on Windows computers

You can install the Symantec Management Agent with a manual push or a manual pull. Symantec recommends that you install the Symantec Management Agent by manually pushing to selected computers. However, to install on the remote computers that have limited network access or are behind a firewall, you may need to perform a manual pull.

See [“About the Symantec Management Agent”](#) on page 201.

Table 17-2 Process for installing the Symantec Management Agent on Windows computers

Step	Action	Description
Step 1	Verify that the computers meet the installation prerequisites.	<p>Each computer must meet the hardware prerequisites and the software prerequisites before you can install the Symantec Management Agent on it.</p> <p>See “Symantec Management Agent for Windows installation prerequisites” on page 208.</p>
Step 2	(Optional) Define the agent registration policies.	<p>After you install the Symantec Management Agent, it sends out a registration request to Notification Server to establish trust between the server and the client.</p> <p>The default agent registration policy allows automatic registration of all agents. You can modify the default policy or create custom policies to specify more restrictive rules.</p> <p>See “Creating an agent registration policy” on page 209.</p>
Step 3	Specify the installation settings.	<p>Before you perform manual push or manual pull installation of the Symantec Management Agent, you must specify the installation settings.</p> <p>See “Specifying the Symantec Management Agent for Windows installation settings” on page 210.</p>
Step 4	Install the Symantec Management Agent using the appropriate method.	<p>The preferred method is to push the Symantec Management Agent to the selected computers. However, if any of the computers are behind a firewall or are difficult for Notification Server to access, you can pull the Symantec Management Agent to them.</p> <p>See “Installing the Symantec Management Agent for Windows with a manual push” on page 211.</p> <p>See “Installing the Symantec Management Agent for Windows with a manual pull” on page 213.</p> <p>See “Performing a scheduled installation of the Symantec Management Agent for Windows” on page 214.</p>
Step 5	View the installation status report to verify successful installation.	<p>The installation status report lets you view details of all the manual push installations and scheduled Symantec Management Agent installations that have been attempted. The report does not include details of any pull installations.</p> <p>See “Viewing the installation status report” on page 215.</p>

Table 17-2 Process for installing the Symantec Management Agent on Windows computers
(continued)

Step	Action	Description
Step 6	View and manage the agent registration status to verify successful registration.	The Agent Registration Status report lets you view and manage all registration requests and completed registrations from Symantec Management Agents. See “Viewing and managing the agent registration status” on page 216.

Symantec Management Agent for Windows installation prerequisites

Before you can install Symantec Management Agent, you need to configure the computers and verify that they meet the installation prerequisites.

See [“Methods for installing the Symantec Management Agent”](#) on page 204.

This task is a step in the processes for installing Symantec Management Agent manually on Windows computers.

See [“Installing the Symantec Management Agent on Windows computers”](#) on page 206.

Table 17-3 Symantec Management Agent for Windows installation prerequisites

Prerequisite	Description
Operating system	Symantec Management Platform and Altiris Solutions Support Matrix
Hard disk space	60 MB minimum
RAM	64 MB minimum (128 MB recommended)
Internet Explorer	Version 6.0 or later
Access rights	Local administrator rights
Firewall	The computer must be able to communicate with Symantec Management Platform through the computer’s firewall. Perform any of the following: <ul style="list-style-type: none"> ■ Enable File and Printer Sharing in the firewall settings. ■ Add port UDP 138, TCP 445, TCP 80 (or TCP 443 for HTTPS) and ICMP type 8 as inbound port exceptions. You can add the ports by using a group policy. ■ Turn off the firewall.
Simple file sharing (Windows XP in non-domain only)	For non-domain client computers running Windows XP, you must also disable Use simple file sharing in Folder Options in Windows XP.

Table 17-3 Symantec Management Agent for Windows installation prerequisites (*continued*)

Prerequisite	Description
UAC (Windows Vista and Windows 7 in non-domain only)	For non-domain client computers running Windows Vista or Windows 7, you must also turn off the User Access Control (UAC).

Creating an agent registration policy

Agent registration policies let you automate the agent registration process. An agent registration policy is a set of rules that determine how the incoming registration requests are processed. In the registration request content, Symantec Management Agent sends its host name, MAC address, IP address, FQDN, and logged on user data. The agent registration policy uses the registration request data and the rules that you define within the policy to decide if the request is allowed or blocked.

Warning: The default agent registration policy automatically allows all agents to communicate with Notification Server. You can modify the default policy or create custom policies to restrict the agents that can communicate with Notification Server. If no active policies are available, the status of each incoming registration request is set to pending.

You can view the registration requests in the **Agent Registration Status** report. You can access this report in the Symantec Management Console, under **Reports > Notification Server Management > Registration**.

See [“Viewing and managing the agent registration status”](#) on page 216.

To create an agent registration policy

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, under **Settings**, expand **Agents/Plug-ins > Symantec Management Agent > Settings**.
- 3 Right-click **Registration Policies**, and then click **New > Registration Policy**.
- 4 In the right pane, specify the settings of the agent registration policy as follows:

Rules

Lets you define different types of masks for agent identification using the request data. For example, you can define a host name mask, an IP address mask, and a logged on user name mask.

A single policy can contain unlimited number of masks of any type. During the mask matching process, Notification Server treats different mask types as logical AND operation and similar mask types as logical OR operation.

For example, a policy with the following masks allows registration of all agents that have the name that matches mask "**test" and their IP address is either 10.31.12.1, 10.31.12.2, or any from 255 IP addresses from the 10.31.15.0 subnet:

- Host = *test
- IP=10.31.12.1
- IP=10.31.12.2
- IP=10.31.15.0/24

Note: Asterisk is accepted for all rules except for **IP address**. If you want to specify an IP range in a rule, you must define it with the subnet mask. For example, instead of typing **10.31.15.***, you enter **10.31.15.0/24**.

Actions

Lets you define the rule for complied agent processing with the following options:

- **Allow**
The agents are automatically registered and you do not need to accept them manually.
- **Block**
Requests from these agents are declined.

Note that if two policies are applicable to a registration request, and one of them allows registration and the other blocks it, the blocking policy is applied to the request.

5 Turn on the policy.

At the upper right of the page, click the colored circle, and then click **On**.

6 Click **Save changes**.

Specifying the Symantec Management Agent for Windows installation settings

The installation settings let you specify how the Symantec Management Agent is installed on the client computer. You can set the installation options for a manual Symantec Management Agent push or pull installation. Note that you cannot include these settings in a CSV file when you import computer names.

This task is a step in the processes for installing the Symantec Management Agent on Windows computers.

See [“Installing the Symantec Management Agent on Windows computers”](#) on page 206.

To set the Symantec Management Agent for Windows installation options

- 1 In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
- 2 On the **Agent Install** page, under **Symantec Management Agent Installation**, click **Default Settings**.
- 3 In the **Symantec Management Agent Settings** dialog box, specify the settings that you want, and then click **OK**.

For more information, click the page and then press **F1**.

- 4 On the **Symantec Management Agent Installation** page, click **Save changes**.

Installing the Symantec Management Agent for Windows with a manual push

You can push Symantec Management Agent to any Windows computers. Before you can manually install or uninstall Symantec Management Agent from the **Symantec Management Agent Install** page, you need to choose the target computers. You can enter the computer names manually, choose the computers that have been discovered with resource discovery, or import the computers from a CSV file. The CSV file is a comma-delimited text file. The file includes the DNS names or the IP addresses of the client computers on which you want to install Symantec Management Agent. For Windows computers, the CSV file is a list of computer names or IP addresses that are imported into the **Symantec Management Agent Install** page. Items are interpreted as the names of computers or the IP addresses of computers (for the entries that are in the appropriate format). No spaces are allowed: any item that contains a space is ignored.

Note: You can manually install Symantec Management Agent only on the computers that were discovered using **Domain Resource Discovery** or **Network Discovery**.

This task is a step in the processes for installing the Symantec Management Agent on Windows computers.

See [“Installing the Symantec Management Agent on Windows computers”](#) on page 206.

To install the Symantec Management Agent for Windows with a manual push

- 1 In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
- 2 On the **Symantec Management Agent Install** page, on the **Install Agent** tab, under **Roll out Agent to Computers**, choose the computers on which to install Symantec Management Agent, and then click **Install**.

To manually add a computer. In the text box, type the IP Address, FQDN, name, or name@domain of the computer, and then click **Add**.

When you type **name@domain**, the system splits the name into two and tries to match the existing resource by both fields. If the full match is not found, the rest of the fields are not populated for this entry.

- To choose from the available computers.
- 1 Click **Select Computers**.
 - 2 In the **Select Computers** dialog box, add the appropriate computers from the **Available computers** list to the **Selected computers** list, and then click **OK**.

- To import computers from a CSV file.
- 1 Under **Roll out Agent to Computers**, on the toolbar, click the **Import computers from a selected file** symbol.
 - 2 In the **Select file to import** dialog box, choose the appropriate CSV file, and then click **Open**.

- 3 (Optional) Under **Roll out Agent to Computers**, using the icons on the toolbar, you can do the following:

View or edit a selected entry.	Select the computer in the list and click the Edit icon. In the Edit entry dialog box, the fields under the Entry fields section are editable and let you update the data in the AgentPushData table. The fields under the Resolved fields section are automatically filled with the data of a matched entry in database. These fields are not editable.
Rediscover the selected entries.	Select the computers in the list, and then click the Rediscover selected computer details icon. Rediscovering lets you search for additional information about the selected computers. For example, domain, operating system details, etc.
View different selections of entries in the grid.	In the View drop-down list, click the selection that you want to view. You can view the computers that are manually added, the computers that are automatically added when the Scheduled Push to Computers is enabled, or both.

- 4 In the **Symantec Management Agent Installation Options** dialog box, configure the installation settings according to your needs, and then click **Proceed With Install**.

For more information, click the page and then press **F1**.

On the **Symantec Management Agent Install** page, under **Roll out Agent to Computers**, in the computer list, the **Status** column shows the success or failure of the installation on each computer. Note that the newly installed Symantec Management Agent reports its status back to the originating Notification Server, even if it is going to be managed by another Notification Server.

Installing the Symantec Management Agent for Windows with a manual pull

If you want to install the Symantec Management Agent on the remote computers that have limited network access, or are behind a firewall, you may need to pull the Symantec Management Agent to each computer. You can log on to each computer, access Notification Server through a URL, and start the Symantec Management Agent installation process. The installation process then runs automatically, with no further user interaction required.

See [“About the Symantec Management Agent”](#) on page 201.

The Symantec Management Agent pull installation uses the settings that are specified in the **Symantec Management Agent Installation Options** dialog box, except for **Download agent package from closest Package Server**, which is irrelevant.

This task is a step in the processes for installing the Symantec Management Agent on Windows computers.

See [“Installing the Symantec Management Agent on Windows computers”](#) on page 206.

To install the Symantec Management Agent for Windows with a manual pull

- 1 Log on to the computer as an administrator.

You can log on remotely using a remote access application, or you can let the user at the remote site log on with the appropriate account.

- 2 On the remote computer, open Internet Explorer and go to the following URL:

`http://NSName/Altiris/NS/Agent/AltirisAgentDownload.aspx`

where *NSName* is the name of your Notification Server computer.

- 3 In the **Symantec Management Agent Download** window, click **Click here to begin download and install**.

A pop-up appears, prompting you to run, save or cancel the installation. If you click **Run**, the agent installation process runs silently and no further action is required.

Performing a scheduled installation of the Symantec Management Agent for Windows

You can configure a scheduled Symantec Management Agent installation. A scheduled installation is performed at a defined time, unlike manual push installations, which are performed immediately. For example, if you want to install the agent on a particular group of computers at a suitable time, you could set up a no repeat schedule to run at the appropriate time.

You can also configure a schedule to automatically install the Symantec Management Agent on new computers as they are added to your environment. The resource discovery schedule runs daily to detect new computers, and you can configure filters to sort the new computers into the appropriate groups. You can then schedule Symantec Management Agent installation on all computers in particular groups at appropriate intervals.

You need to be careful when you implement an automatic installation method. Symantec recommends that you include a manual step to verify that the agent is installed on the appropriate computers.

This task is a step in the processes for installing the Symantec Management Agent on Windows computers.

See [“Installing the Symantec Management Agent on Windows computers”](#) on page 206.

To configure the Symantec Management Agent for Windows installation schedule

- 1 In the **Symantec Management Console**, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
- 2 On the **Symantec Management Agent Install** page, under **Scheduled Push to Computers**, at the right of the page, click the colored circle, and then click **On**.
- 3 Under **Apply To**, specify the computers on which the Symantec Management Agent is to be installed.

You can specify an existing organizational group, filter, or resource target. You can also select individual resources.
- 4 Under **When to Schedule** panel, specify the scheduled time or schedule window to perform the installation and select the appropriate options.
- 5 Click **Save changes**.

Viewing the installation status report

The installation status report lets you view details of all of the Symantec Management Agent push installation attempts that have been made. The report does not include details of any pull installations.

By default, details of all installation attempts that were made in the past week are listed. You can specify the period to view and filter the results by computer name and domain.

This task is a step in the following processes:

- Installing the Symantec Management Agent on Windows computers.
See [“Installing the Symantec Management Agent on Windows computers”](#) on page 206.
- Installing the Symantec Management Agent manually on UNIX, Linux, and Mac computers.
See [“Installing the Symantec Management Agent on UNIX, Linux, and Mac computers”](#) on page 219.

To view the Agent Installation Status report

- 1 In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
- 2 On the **Symantec Management Agent Install** page, click **Status Report**.

The report shows details of all push installation attempts for the Symantec Management Agent and the Symantec Management Agent for UNIX, Linux, and Mac. The same report is available from both the **Install Agent** and the **Install Agent for UNIX, Linux, and Mac** tabs.
- 3 In the **Agent Installation Status** window, view the details of each installation attempt.

- 4 (Optional) If you want to change the time period or filter the results by computer name and domain, under **Parameters**, set the appropriate user parameters:

Showing	Specify the time period that you want to view. Type the appropriate number of units (hours, days, weeks, or months) in the From and To boxes.
Units	Specify the units that you want to use for the Showing values.
Filter By	If you want to filter the results by computer name or domain (or both), specify the appropriate filter text in the corresponding boxes.

- 5 (Optional) If you have changed the user parameters, click **Refresh** to display the updated report results.

Viewing and managing the agent registration status

The **Agent Registration Status** report lets you view all registration requests and completed registrations from Symantec Management Agents.

In this report, you can see the computers that the **Agent Registration Policy** has automatically allowed or blocked. Note that for direct Symantec Management Agent push installation, the registration is bypassed. However, the computers are still displayed in the report and their status is set to **Allowed**. If no **Agent Registration Policy** applies to the computer, its status is set to **Pending** and the right-click menu lets you manually allow or block it. The right-click menu also lets you revoke the trust of the agents that you have previously allowed.

See [“Creating an agent registration policy”](#) on page 209.

Incoming registration requests are distinguished by the resource keys and they are merged based on the resource keys lookup.

In some situations, duplicate registration requests may appear. For example, if you reinstall the agent on a computer that is already registered on Notification Server, its public key changes. In this case, Symantec recommends that you approve the registration request to let this computer continue communicating with Notification Server. Also, the duplicate registration requests may appear if you have computers with identical resource keys in your network. In this case, Symantec recommends not to approve the duplicate registration request because it may cause connectivity issues for the resource that previously existed.

If you have duplicate registration requests in your report, the requests are handled as follows:

- If the initial request is allowed and the duplicate request is also allowed, the duplicate request is merged with the existing resource and the report is updated to display a single entry.
- If the initial request is allowed but the duplicate request is blocked, both requests remain in the list. The allowed request represents the actual resource and the duplicate request

in blocked or pending state represents the registration attempt from a potentially duplicated resource.

The **Agent Registration Status** report keeps all requests for audit purposes and lets you continuously observe them.

To view and manage the agent registration status

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, under **Reports**, expand **Notification Server Management > Registration**, and then click **Agent Registration Status**.
- 3 (Optional) On the **Agent Registration Status** page, use the right-click menu options to modify the status of the agent. Note that depending on the status of the agent, the right-click options vary.

Allow You can allow the agents that are in the **Pending**, **Blocked**, or **Revoked** state. If you allow a blocked agent, the trust is granted next time when the agent sends a registration request to Notification Server.

Block You can block the agents that are in the **Pending** or **Revoked** state. If you block a revoked computer, its functional status does not change. However, changing the status lets you differentiate the revoked computers that should never again connect to Notification Server from the revoked computers that may still require your attention. Note that computers with the **Blocked** status are removed from the list after a predefined period of time if no new registration requests were sent from the same computer during this time. The default period is three months, but you can change it on the **Purging Maintenance** page.

Revoke You can revoke the registration of the agents that you have previously allowed. For example, you can revoke the registration for the client computer that is reported missing or stolen. After you revoke the agent, it stops receiving policies from Notification Server. Also, a revoked computer cannot be used as a site server.

During the revocation of internal agent trust, the agent encryption key registration gets marked as revoked on Notification Server. Revoked agents do not receive policies and do not run tasks. Also, the revoked agent clears locally stored policies to minimize its activity. After the revocation, Symantec Management Agent is forced to reinitiate the registration process.

The agent receives information about its revoked status next time when it tries to access secured data. Notification Server does not notify the agent about the revocation event when it occurs.

Note that the revoked agent remains in the **Revoked** state even if the agent registration policy allows it. You must manually manage the revoked computers, if you want to change their state.

Installing the Symantec Management Agent on UNIX, Linux, and Mac computers

You can install the Symantec Management Agent with a manual push or a manual pull. It is recommended to install the Symantec Management Agent by manually pushing to selected computers. However, to install on the remote computers that have limited network access or are behind a firewall, you may need to perform a manual pull.

See [“About the Symantec Management Agent”](#) on page 201.

Table 17-4 Process for installing the Symantec Management Agent on UNIX, Linux, and Mac computers

Step	Action	Description
Step 1	Select the computers to which you want to install the agent and plug-ins.	<p>You have the following options for selecting computers:</p> <ul style="list-style-type: none"> ■ Network Discovery ■ Manual selection by adding client host names or IP addresses ■ Active Directory Import ■ Import using a comma-separated values file.
Step 2	Verify that the computers meet the installation prerequisites.	<p>Each computer must meet the hardware prerequisites and the software prerequisites before you can install the Symantec Management Agent on it.</p> <p>See “Symantec Management Agent for UNIX, Linux, and Mac installation prerequisites” on page 221.</p>
Step 3	(Optional) Define the agent registration policies.	<p>After you install the Symantec Management Agent, it sends out a registration request to Notification Server to establish trust between the server and the client.</p> <p>The default agent registration policy allows automatic registration of all agents. You can modify the default policy or create custom policies to specify more restrictive rules.</p> <p>See “Creating an agent registration policy” on page 209.</p>
Step 4	Specify the installation settings.	<p>The UNIX, Linux, and Mac installation settings let you configure the communication and the authentication settings for the Symantec Management Agent for UNIX, Linux, and Mac. If you import computer names from a CSV file, you can specify these settings in the CSV file. You can also set or change these settings from the Symantec Management Console.</p> <p>See “Specifying the Symantec Management Agent for UNIX, Linux, and Mac installation settings” on page 222.</p>

Table 17-4 Process for installing the Symantec Management Agent on UNIX, Linux, and Mac computers (*continued*)

Step	Action	Description
Step 5	Install the Symantec Management Agent using the appropriate method.	The preferred method is to push the Symantec Management Agent to the selected computers. However, if any of the computers are behind a firewall or are difficult for Notification Server to access, you can pull the Symantec Management Agent to them. See “Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual push” on page 223. See “Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual pull” on page 226.
Step 6	View and manage the agent registration status to verify successful registration.	The Agent Registration Status report lets you view and manage all registration requests and completed registrations from Symantec Management Agents. See “Viewing and managing the agent registration status” on page 216.

Creating a CSV file for importing UNIX, Linux, and Mac computers

If you want to install the Symantec Management Agent for UNIX, Linux, and Mac on a large number of computers that require different connection and configuration settings, use a CSV file to import the computers and configure the installation settings. The CSV file is a comma-delimited text file that includes the DNS names or the IP addresses of the client computers on which you want to install the Symantec Management Agent. Each line in the CSV file represents a computer entry that is imported into the **Symantec Management Agent Install** page. The CSV file can also contain the installation settings for each computer.

See [“Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual push”](#) on page 223.

A CSV template file for importing UNIX, Linux, and Mac computers (`CSVTemplate.csv`) is provided with the Symantec Management Platform. The column header of the CSV template indicates the data that is required and the valid values that you can use.

Warning: The CSV file format (list separator) must meet the regional settings of the server. For example, the sample `CSVTemplate.csv` file uses the "English (United States)" regional settings with a comma "," as a list separator. You can view the Symantec Management Platform's regional settings in the Windows **Control Panel**.

This task is a step in the process for installing the Symantec Management Agent manually.

See [“Installing the Symantec Management Agent on Windows computers”](#) on page 206.

To create a CSV file for importing UNIX, Linux, and Mac computers

- 1 In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
- 2 On the **Symantec Management Agent Install** page, on the **Install Agent for UNIX, Linux and Mac** tab, under **Push install**, right-click **CSV file template**, and then click **Save Target As**.
- 3 In the **Save As** dialog box, type a suitable file name for the `CSVTemplate.csv` file, browse to the appropriate location, and then click **Save**.
- 4 Open the saved CSV file in a text editor and enter the information for each computer on which you want to install the Symantec Management Agent for UNIX, Linux, and Mac.

You do not have to use all of the fields. You can use only the fields that you need, such as computer name, root name, root password, and so on.

The settings that you can specify in the CSV file are identical to the settings that you can set from the **Install Settings** window in the Symantec Management Console.

- 5 When you have finished, save the CSV file.

Symantec Management Agent for UNIX, Linux, and Mac installation prerequisites

Your computer must meet the hardware and software prerequisites before you can install the Symantec Management Agent for UNIX, Linux, and Mac.

See [“Methods for installing the Symantec Management Agent”](#) on page 204.

This topic is a step in the process for installing the Symantec Management Agent manually.

See [“Installing the Symantec Management Agent on Windows computers”](#) on page 206.

Table 17-5 Symantec Management Agent for UNIX, Linux, and Mac installation prerequisites

Prerequisite	Description
Operating system	Symantec Management Platform and Altiris Solutions Support Matrix
Hard disk space	60 MB minimum
RAM	25 MB minimum
Access rights	Root user or a user with administrative privileges is required on UNIX/Linux and Mac platform.

Table 17-5 Symantec Management Agent for UNIX, Linux, and Mac installation prerequisites
(continued)

Prerequisite	Description
Remote SSH connections enabled	Remote SSH connections must be enabled. There must be an SSH server running on the client computer and the firewall must be configured to allow an incoming SSH connection.
Outgoing connection to Notification Server enabled	The firewall must be configured to allow an outgoing connection to a WEB port on Notification Server.

Specifying the Symantec Management Agent for UNIX, Linux, and Mac installation settings

The Symantec Management Agent installation settings are the communication and the authentication settings for the Symantec Management Agent for UNIX, Linux, and Mac. You must specify the appropriate privileged account login name and password for each target computer.

See [“Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual push”](#) on page 223.

When you import computers from a CSV file, you can specify the appropriate installation settings for each computer in the CSV file. If you do not specify any settings in the CSV file, or if you added computers manually, you need to specify the appropriate settings for each target computer before you install the Symantec Management Agent for UNIX, Linux, and Mac.

You can specify installation settings for a particular computer or for multiple computers. If you select multiple computers, the same installation settings are applied to each computer. You can also clone the current installation settings from a computer and apply it to other computers.

See [“Creating a CSV file for importing UNIX, Linux, and Mac computers”](#) on page 220.

This task is a step in the process for installing the Symantec Management Agent manually.

See [“Installing the Symantec Management Agent on Windows computers”](#) on page 206.

To specify the Symantec Management Agent for UNIX, Linux, and Mac installation settings

- 1 In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
- 2 On the **Symantec Management Agent Install** page, on the **Install Agent for UNIX, Linux and Mac** tab, under **Push install**, in the computer list, click the computer for which you want to change the Symantec Management Agent installation settings, and then click **Installation Settings**.

If you want to specify identical installation settings for multiple computers, or if you want to clone the current installation settings from another computer, select the appropriate computers.

- 3 (Optional) If you want to clone the current installation settings from a particular computer, in the **Installation Settings** dialog box, in the **Load settings** drop-down list, select the appropriate computer.

The option **Load settings of** appears at the upper right of the **Installation Settings** dialog box if you have selected multiple computers.

- 4 Specify the appropriate installation settings for the selected computers.

For more information, click the page and then press **F1**.

- 5 In the **Installation Settings** dialog box, click **OK**.

Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual push

You can push the Symantec Management Agent for UNIX, Linux, and Mac to any of the computers that are listed in the Symantec Management Agent Install page.

Before you can manually install the Symantec Management Agent from the **Symantec Management Agent Install** page, you need to select the appropriate computers. You can select the computers that have been discovered with resource discovery, enter the computer names manually, or import the computers from a CSV file.

The push installation of the Symantec Management Agent for UNIX, Linux, and Mac is performed by the Symantec Management Platform computer. The Symantec Management Platform computer establishes a connection to the target UNIX, Linux, or Mac computer, uploads the required files, and then executes them on the target computer.

The installation process is as follows:

- The Symantec Management Platform attempts to connect to the target computer through SSH.

The SSH protocol supports logon with either privileged or unauthorized user accounts and multiple passwords.

- When connection is established, the Symantec Management Platform determines the client computer's operating system and environment, and then it launches the appropriate platform-specific push-install script.
- The push-install script creates a directory structure on the client computer, and then it attempts to download the `aex-bootstrap` utility from the Symantec Management Platform computer. The push-install script tries each of the following methods, in order, until one succeeds: SCP/SFTP, `wget`, `curl`.
 If all of these methods fail, the script uses `dd` command to transfer the `aex-bootstrap.Z.uu` archive to the target computer. It then uses `uudecode` to convert the archive to a native format.
- The `.aex-agent-install-config.xml` file that contains all of the Symantec Management Agent installation settings is downloaded to the client computer.
- The `aex-bootstrap` script is executed, and the connection to Symantec Management Platform is closed.
- The `aex-bootstrap` script downloads the `res.aex-agent-install-config.xml` of the Symantec Management Agent from the Symantec Management Platform computer and configures the Symantec Management Agent with settings from the file.
- When the Symantec Management Agent for UNIX, Linux, and Mac runs for the first time, it collects basic inventory and posts it to the Symantec Management Platform.
- The Symantec Management Agent for UNIX, Linux, and Mac receives the appropriate tasks and policies from the Symantec Management Platform.

Note: Third-party firewalls must be configured to allow an SSH connection from Symantec Management Platform to the ULM client for a manual push to work. The firewalls configuration should use the same credentials that you provide in the **Installation Settings** dialog box in step 4.

This task is a step in the process for installing the Symantec Management Agent manually.

See [“Installing the Symantec Management Agent on Windows computers”](#) on page 206.

To install the Symantec Management Agent for UNIX, Linux, and Mac with a manual push

- 1 In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
- 2 On the **Symantec Management Agent Install** page, on the **Install Agent for UNIX, Linux, and Mac** tab, under **Push install**, select the UNIX, Linux, and Mac computers on which to install the Symantec Management Agent:

To manually add a computer In the text box, type the computer name (which must be a DNS-resolvable name) or IP address and then click **Add**.

To select from the available computers Click **Select Computers**, in the **Select Computers** dialog box, add the appropriate computers from the **Available computers** list to the **Selected computers** list, and then click **OK**.

To import computers from a CSV file **1** In the toolbar, click **Import computers from a selected file**.
2 In the **Select File to Import** dialog, select the appropriate CSV file, and then click **Open**.

The CSV file is a comma-delimited text file. The file includes the DNS names or the IP addresses of the client computers on which you want to install the Symantec Management Agent. For UNIX, Linux, and Mac computers, each line in the CSV file represents a computer entry that is imported into the **Symantec Management Agent Install** page. You can also include the appropriate installation settings in the CSV file. These installation settings let you configure the communication and the authentication settings for the Symantec Management Agent for UNIX, Linux, and Mac.

If you have a large number of computers that require different connection and configuration settings, use a CSV file to import the computers.

See [“Creating a CSV file for importing UNIX, Linux, and Mac computers”](#) on page 220.

3 Click **Installation Settings**, and then in the **Installation Settings** dialog box, specify the appropriate installation settings.

If you added computers manually, you need to specify the appropriate installation settings for each target computer before you install the Symantec Management Agent for UNIX, Linux, and Mac. If you imported computers from a CSV file, you may have specified the installation settings for each computer in the CSV file. You can change these settings for individual computers or groups of computers.

See [“Specifying the Symantec Management Agent for UNIX, Linux, and Mac installation settings”](#) on page 222.

4 (Optional) In the **Simultaneous Tasks** box, specify the number of installations to run simultaneously.

This value defines the number of threads running in parallel and serving Symantec Management Agent pushing. All of the threads share a common queue from which they take the next computer to install to. The default value is 5, but you may want to use a different value to suit the performance of the Symantec Management Platform, the client computers, and the network capacity. Increasing the number of simultaneous tasks may reduce the total installation time.

5 Click **Install**.

- 6 In the **Push install** dialog box, click **OK**.

The **Status** column in the computer list shows the success or failure of the installation on each computer. Note that the newly installed Symantec Management Agent reports its status back to the originating Notification Server, even if another Notification Server manages it.

- 7 If the computer list does not refresh automatically, in the toolbar, click **Refresh** to view the current push installation status for each computer.

Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual pull

If SSH is not available, or if you want to install the Symantec Management Agent for UNIX, Linux, and Mac on remote the computers that have limited network access, or the target computers are behind a firewall, you can pull the Symantec Management Agent to each computer. You, or anybody else with administrator rights, can log on to each computer, access Symantec Management Platform through a URL, and download the install bootstrap program that performs the Symantec Management Agent for UNIX, Linux, and Mac installation.

The URL of the **Download Symantec Management Agent for UNIX, Linux and Mac** page is shown on the **Symantec Management Agent Install** page, under **Download Page URL for UNIX, Linux and Mac**. You can view the page, but you cannot change this setting.

See [“About the Symantec Management Agent”](#) on page 201.

See [“Symantec Management Agent for UNIX, Linux, and Mac troubleshooting commands”](#) on page 439.

This task is a step in the process for installing the Symantec Management Agent manually.

See [“Installing the Symantec Management Agent on Windows computers”](#) on page 206.

To preview the **Download Symantec Management Agent for UNIX, Linux and Mac** page

- 1 In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
- 2 On the **Symantec Management Agent Install** page, on the **Install Symantec Management Agent for UNIX, Linux and Mac** tab, under **Download Page URL for UNIX, Linux and Mac users**, in the **Select platform** drop-down list, click the appropriate platform, and then click **View page**.

To pull the Symantec Management Agent for UNIX, Linux and Mac to a remote computer

- 1 Log on to the remote computer as an administrator.
- 2 On the remote computer, open a Web browser , and then go to the following URL:
`http://SMPName/Altiris/UnixAgent/AltirisUnixAgentDownload.aspx?ID=Platform`
where *SMPName* is the name of your Symantec Management Platform computer and *Platform* is the appropriate platform.
- 3 Follow the instructions that are displayed on the **Download Symantec Management Agent for UNIX, Linux and Mac** page for downloading and running the install bootstrap program on the remote computer.

Upgrading and uninstalling the Symantec Management Agent

This chapter includes the following topics:

- [Methods for upgrading the Symantec Management Agent](#)
- [Methods for uninstalling the Symantec Management Agent](#)
- [Configuring the Symantec Management Agent Upgrade and Uninstall policies](#)
- [Configuring the Symantec Management Agent package](#)
- [Removing the Symantec Management Agent for Windows manually](#)

Methods for upgrading the Symantec Management Agent

You need to install the appropriate version of the Symantec Management Agent on your managed computers. If any computers have old versions of the agent installed, you should upgrade them.

See [“About the Symantec Management Agent”](#) on page 201.

Table 18-1 Symantec Management Agent upgrade methods

Method	Description
Manually push the Symantec Management Agent to the appropriate computers.	<p>You can upgrade the Symantec Management Agent manually by pushing it to the appropriate computers. You can push to a computer that has an older version of the Symantec Management Agent installed.</p> <p>See “Installing the Symantec Management Agent for Windows with a manual push” on page 211.</p> <p>See “Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual push” on page 223.</p>
Use the Symantec Management Agent upgrade policy.	<p>The Symantec Management Agent upgrade policy is provided with Notification Server. You can turn on this policy and configure it to ensure that all of your managed computers have the correct Symantec Management Agent version installed.</p> <p>See “Configuring the Symantec Management Agent Upgrade and Uninstall policies” on page 230.</p>

For more information about upgrading Symantec Management Agent, see the *IT Management Suite Installation and Upgrade Guide*.

Methods for uninstalling the Symantec Management Agent

You can remove the Symantec Management Agent from a managed computer when you no longer need it. You do not need to remove any solution agents that have been installed on the computer, as they are removed automatically as part of the Symantec Management Agent uninstallation process.

See [“About the Symantec Management Agent”](#) on page 201.

Table 18-2 Methods for uninstalling the Symantec Management Agent

Method	Description
Manual uninstallation.	<p>Manual uninstallation is initiated from the Symantec Management Console and removes the Symantec Management Agent immediately. You can remove the Symantec Management Agent from any number of Windows computers in the same uninstall operation. You can also customize the uninstallation options for each operation.</p> <p>This option is available for Windows computers only.</p> <p>See “Removing the Symantec Management Agent for Windows manually” on page 233.</p>
Use the Symantec Management Agent uninstall policy.	<p>The Symantec Management Agent uninstall policy is provided with Symantec Management Platform. You can turn on this policy and configure it to ensure that the Symantec Management Agent is removed from the appropriate computers.</p> <p>This option is available both for Windows computers and for UNIX, Linux, and Mac computers.</p> <p>See “Configuring the Symantec Management Agent Upgrade and Uninstall policies” on page 230.</p>

Configuring the Symantec Management Agent Upgrade and Uninstall policies

You can configure the Symantec Management Agent upgrade and Symantec Management Agent uninstall policies to suit your requirements. Both policies use the appropriate Symantec Management Agent package but use different programs.

See [“About the Symantec Management Agent”](#) on page 201.

Notification Server provides some default filters that you can use in the scheduled agent installation operations, and in agent upgrade and agent uninstall policies. These filters are stored in the Symantec Management Agent folder, under the appropriate subfolder. You cannot modify the default filters, but you can clone them to create the new filters that you can edit to suit your requirements.

However, you must be careful when you perform Symantec Management Agent upgrades based on resource targets. In a large environment you may prefer to stagger the upgrades by using a trial target first, and then a staggered rollout through suitable targets, rather than perform them all at the same time. For example, there may be some issues with the upgrade, so you can test it on a small number of computers and identify and resolve the problems without affecting every computer. A staggered upgrade also helps to manage the load on the network

as the agents typically need to request data from Notification Server as soon as they are upgraded.

To configure the agent upgrade and uninstall policies

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Settings > Agents/Plug-ins > Symantec Management Agent**, and then perform one of the following actions:

To configure the Symantec Management Agent upgrade policy.

- For Windows x64 computers, expand **Windows > Non Site Server**, and then click **Symantec Management Agent for Windows x64 (Non-Site Server) - Upgrade to 64-bit Symantec Management Agent**.
- For Windows x86 computers, expand **Windows > Non Site Server**, and then click **Symantec Management Agent for Windows x86 (Non-Site Server) - Upgrade to 32-bit Symantec Management Agent**.

To configure the policy that upgrades the Symantec Management Agent on the computers that contain one or more site services.

- For Windows x64 computers, expand **Windows > Site Server**, and then click **Symantec Management Agent for Windows x64 (Site Server Only) - Upgrade to 64-bit Symantec Management Agent**.
- For Windows x86 computers, expand **Windows > Site Server**, and then click **Symantec Management Agent for Windows x86 (Site Server Only) - Upgrade to 32-bit Symantec Management Agent**.

To configure the Symantec Management Agent uninstall policy.

Expand the **Windows** folder, and then click **Symantec Management Agent for Windows - Uninstall**.

To configure the Symantec Management Agent for UNIX/Linux/Mac upgrade policy.

Expand the **UNIX/Linux/Mac** folder, and then click **Symantec Management Agent for UNIX/Linux/Mac - Upgrade**.

To configure the Symantec Management Agent for UNIX/Linux/Mac uninstall policy.

Expand the **UNIX/Linux/Mac** folder, and then click **Symantec Management Agent for UNIX/Linux/Mac - Uninstall**.

3 In the right pane, make the appropriate configuration changes:

Program name	The name of the Symantec Management Agent package program that is run when the policy is triggered. The default setting is the program that is appropriate to the policy, and you should not need to change it. However, if you have added a new program to the Symantec Management Agent package, you may want to use that instead.
Enable Verbose Reporting of Status Events	<p>Enable the sending of package status events to Notification Server.</p> <p>The Notification Server Event Capture settings in the Global Symantec Management Agent Settings policy take precedence over the Enable Verbose Reporting of Status Events setting here. Events are sent only if they are enabled in the Global Symantec Management Agent Settings policy.</p> <p>See “Configuring the global agent settings” on page 236.</p>
Applied to	<p>Specify the computers to which the policy applies.</p> <p>You can use the predefined filters that are supplied with Notification Server or create your own.</p>
Package Multicast	<p>Disables the package download through multicast.</p> <p>Multicast typically slows down the rollout of a package, so you may want to turn it off for an urgent patch. Additionally, in some environments multicast does not work. For example, it may be disabled at routers and switches.</p> <p>The Package Multicast settings in the Global Symantec Management Agent Settings policy take precedence to the settings here.</p>
Schedule	<p>Specify the policy schedule.</p> <p>See “Specifying a policy schedule” on page 326.</p>

4 Turn on the policy.

At the upper right of the page, click the colored circle, and then click **On**.

5 Click **Save changes**.

Configuring the Symantec Management Agent package

The Symantec Management Agent installation policies use the appropriate Symantec Management Agent package when you upgrade or uninstall an agent. Symantec recommends not changing any settings in this package.

After you configure a Symantec Management Agent package, you need to update the package distribution points to update the package information on each package server.

See [“Updating the distribution points for a package”](#) on page 318.

To configure the Symantec Management Agent package

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Settings > Agents/Plug-ins > Symantec Management Agent**.
- 3 In the **Windows** or **UNIX/Linux/Mac** folder, click the Symantec Management Agent package that you want to configure.
- 4 On the **Symantec Management Agent Package** page, make the necessary configuration changes on the appropriate tabs.

For more information, click the page and then press **F1**.

- 5 Click **Save changes**.

Removing the Symantec Management Agent for Windows manually

You can manually remove the Symantec Management Agent from any of the computers that you select.

To remove the Symantec Management Agent manually

- 1 In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
- 2 On the **Symantec Management Agent Install** page, select the Windows computers from which to remove the Symantec Management Agent.
- 3 On the **Symantec Management Agent Install** page, under **Roll out Agent to Computers**, click **Uninstall**.

- 4 In the **Symantec Management Agent Uninstall Options** dialog box, check the options that you want to use, and specify the necessary settings in the appropriate boxes.

Use proxy (if configured on target computer) Use this option if the computer that you push needs to connect to Notification Server through a proxy server. The same proxy settings are used to connect to Notification Server as the proxy settings that are used by Internet Explorer.

Use the following admin account An administrator account is needed to start the uninstall service on the computer from which the Symantec Management Agent is removed. By default Notification Server application identity is used. If this account does not have permission to access the computer, another account needs to be used.

You need to specify the appropriate administrator account user name and password to use.

- 5 Click **Proceed with Uninstall**.

Configuring the Symantec Management Agent

This chapter includes the following topics:

- [Configuring the Symantec Management Agent using the configuration policies](#)
- [Configuring a Notification Server communication profile](#)
- [Redirecting the Symantec Management Agent to communicate with a different Notification Server](#)

Configuring the Symantec Management Agent using the configuration policies

The default Symantec Management Agent configuration settings are suitable for a small Symantec Management Platform environment. As your environment grows, or if your organization has particular requirements, you need to make the appropriate configuration changes.

The agent configuration settings are applied to the appropriate managed computers using agent configuration policies. You can modify these policies to change the settings at any time. The new configuration settings are applied to the agents when the managed computers get their next policy updates (which is typically once a day).

Table 19-1 Types of agent configuration policies

Type	Description
Global settings	The global configuration settings apply to all Symantec Management Agents on all managed computers. These settings are applied as a single policy that automatically targets every managed computer. See “Configuring the global agent settings” on page 236.
Targeted settings	The targeted agent settings are the general parameters that control the Symantec Management Agent, including how the agent communicates with Notification Server. You can modify the default policies that are supplied with the Symantec Management Platform. You can create your own targeted agent settings policies and apply them to the appropriate managed computers. See “Configuring the targeted agent settings” on page 237.
Maintenance windows	A maintenance window is a scheduled time and duration when maintenance operations may be performed on a managed computer. A maintenance window policy defines one or more maintenance windows. You can modify the default policy that is supplied with the Symantec Management Platform. You can create your own maintenance window policies and apply them to the appropriate managed computers. See “Configuring maintenance window policies” on page 244.

The targeted settings policies and maintenance window policies are applied to the managed computers that are included in the specified policy targets. These targets may not be mutually exclusive. Two or more policies of the same type may apply to the same managed computer.

Configuring the global agent settings

The global configuration settings are those that you would not need to set differently on different computers, so they apply to all Symantec Management Agents on all managed computers. These settings are applied as a global agent settings policy, so they are updated in the same way as any other policy. By default, the global agent settings policy is refreshed hourly. You cannot delete or disable the global agent settings policy, or create alternative versions of it.

If you want to specify agent settings for particular groups of managed computers, you need to configure the appropriate targeted agent settings policies.

To configure the global agent settings

- 1 In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Global Settings**.
- 2 Make the appropriate configuration settings on the following tabs:

General	Specify the Tickle/Power Management and Package Multicast settings.
Authentication	Specify the user name and password that the Symantec Management Agent uses when it connects to Notification Server or to a package server.
Events	Specify Notification Server events that you want to capture.

For more information, click the page and then press **F1**.

- 3 Click **Save changes**.

See [“Configuring the Symantec Management Agent using the configuration policies”](#) on page 235.

Configuring the targeted agent settings

The targeted agent settings let you configure the general parameters that control the Symantec Management Agent, including how the agent communicates with Notification Server. You can apply these settings to particular groups of computers. For example, some groups of computers may have different purposes, or you may want to treat servers differently from other managed computers. You can modify the default policies that are supplied with Notification Server or create your own targeted agent settings policies.

Note: The **(Initial Settings)** policy lets you send the initial set of settings to the agents of client computers that have successfully registered on Notification Server but not yet appeared in the target of any regular **Targeted Agent Settings** policy. For example, after a re-imaged client computer receives the **(Initial Settings)** policy with Agent Connectivity Credentials, it can immediately connect to Task Server.

The **(Initial Settings)** policy has no specific target because it is automatically applied to the registered agents that are not found in the target of any other **Targeted Agent Settings** policy. After the agent appears in the target of a regular **Targeted Agent Settings** policy, it receives the settings of the regular policy.

Note that if you clone the **(Initial Settings)** policy, it will become a regular policy and is applied based on the configured target.

If you want to specify some configuration settings that apply to all Symantec Management Agents on all managed computers, you need to configure the global agent settings policy.

To configure the targeted agent settings

- 1 In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Targeted Agent Settings**.
- 2 In the left pane, do one of the following:
 - To create a new **Targeted Agent Settings** policy, click **Create new**.
 - To set or change the policy name, click the appropriate policy, and then click **Rename**. In the **Rename Item** dialog box, type the new name, and then click **OK**.
- 3 In the right pane, make the appropriate configuration settings on the following tabs:

General	General settings include the policy download and inventory collection frequencies, and the computers, users, or resource targets to which the policy applies.
UNIX/Linux/Mac	Provides general settings for UNIX, Linux, and Mac managed computers.
Downloads	Download settings control how each agent downloads packages during software deliveries. You can define throttling or enable and configure multicast download or peer-to-peer downloading. See “Configuring the settings for peer-to-peer downloading” on page 239. Note that you can override the global multicast settings for individual software delivery policies and tasks.
Blockouts	Blockout periods are times when all communication between the agent and Notification Server is disabled. You can set up any number of blockout periods.
User Control	The user control settings are the options that affect what the user of the managed computer can see.
Advanced	Lets you specify an alternate URL that the Symantec Management Agent can use to access Notification Server, install SSL certificates on managed computers, and turn on the power management feature.
Health Evaluation	Lets you configure how the health of the Symantec Management Agent is evaluated for the Computer view.

For more information, click the page and then press **F1**.

- 4 (Optional) To restore the policy to its default settings, click **Restore Defaults**.
- 5 Click **Save changes**.

See [“Configuring the Symantec Management Agent using the configuration policies”](#) on page 235.

Configuring the settings for peer-to-peer downloading

(Windows only)

The peer-to-peer downloading feature lets you download and distribute the software delivery and patch packages to Windows computers. It minimizes the software delivery time and provides you with a reliable software delivery to all endpoints. The peer-to-peer downloading feature significantly reduces the load on WAN and on IT Management Suite infrastructure.

You can benefit from this feature when distributing Windows cumulative updates and other software packages to your client computers. You can also use this feature when managing the Windows 7, 8, and 10 devices at sites with low-bandwidth connections and no dedicated package servers.

Note: The peer-to-peer downloading feature is not supported in Deployment Solution.

Note that peer-to-peer downloading is different from multicast downloading. The idea of multicast downloading is to temporarily use one regular client computer as a package server which downloads a package from Notification Server and then transmits it to the other client computers. In peer-to-peer downloading, the peer computers find each other, request the information about the packages, and download the package from the peer computer that has the required package available.

Note: You cannot use multicast downloading and peer-to-peer downloading simultaneously.

The concept of peer-to-peer downloading is as follows:

Symantec Management Agent discovers the peers.	After you enable peer-to-peer downloading, Symantec Management Agents discover peers by sending broadcast or unicast HTTP messages and join the Distributed Hash Table (DHT) network.
HTTP server stores the list of packages.	<p>The HTTP server is part of the Symantec Management Agent process. It starts automatically after you enable peer-to-peer downloading.</p> <p>The HTTP server stores the list of package GUID-s with their associated states.</p> <p>The Package Delivery component on Symantec Management Agent informs the HTTP server about the folder where the downloaded packages are stored and about the state of each package.</p>

DHT provides the package information to the peers.

The DHT algorithm uses the list of packages from HTTP server to generate the information for the peers in the DHT network.

When the peers look for a specific package, they look for the state of the package and the location of the package in the DHT network.

Note that Symantec Management Agent looks for all the peers only once during one download attempt.

Package Delivery downloads the packages.

When the Package Delivery must download a package, it first looks for the GUID of the required package in DHT. DHT responds with a list of peer computers where this package is being downloaded or already available.

If the package is being downloaded on one of the peer computers, the Package Delivery retries to download the package from this peer later.

If the package is already available on some peer computers, the Package Delivery attempts to download the package from one of these peers. Once the package is downloaded, the computer changes the state of this package in DHT to "Ready".

When the Package Delivery cannot find the required package on the peer computers, it changes the state of this package in DHT to "Downloading" and starts downloading the package from Package Server or Notification Server. When the download of this package finishes, its state is changed to "Ready".

Peer-to-peer engine uses only HTTP for package transfer.

You configure the peer-to-peer downloading settings in the Symantec Management Console, on the **Targeted Agent Settings** page, on the **Downloads** tab.

To ensure that the peer-to-peer downloading works efficiently, Symantec recommends the following additional configuration:

Keep the packages on the client computer for at least one week.

Peer-to-peer downloading does not function or functions with limitations if you remove the package from the client computer immediately or after a few days.

To avoid this issue, you must configure the **Package files will be deleted from the client computer if unused for** option as required. The suggested minimum period for the package to be stored on the client computer is **1 week**.

You can configure this option in the Symantec Management Console, on the **Symantec Management Agent Package** page.

To access this page, in the Symantec Management Console, on the **Settings** menu, click **All Settings**, and then in the left pane, expand **Settings > Agents/Plug-ins > Symantec Management Agent > Windows**.

Configure a schedule for the installation of the Windows 10 feature updates.

Peer-to-peer downloading does not work efficiently if you configure the Windows 10 feature updates to be installed **ASAP**. In this case, each computer would start installing the feature update right after the package download. During the update installation, the Symantec Management Agent is inactive and not able to distribute the downloaded feature update to its peers. As a result, numerous agents download the feature update directly from Package Server or Notification Server. Symantec recommends setting specified time for the update installation to give computers enough time to distribute downloaded feature update to their peers.

You can configure this option in the Symantec Management Console, on the **Software Management Solution Plug-in Install** page.

To access this page, in the Symantec Management Console, on the **Settings** menu, click **All Settings**, and then in the left pane, expand **Agents/Plug-ins > Software > Software Management**.

Alternatively, you can configure this option for the specific software update policy.

To configure the settings for peer-to-peer downloading

- 1 In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Targeted Agent Settings**.
- 2 In the left pane, select the policy for which you want to configure the peer-to-peer downloading settings.

- 3 In the right pane, on the **Downloads** tab, under **Peer-to-peer Downloading Settings**, configure the settings.

Note that the default settings are suitable for most of the environments. However, if you notice too many direct downloads or long package delivery period, you may need to customize the settings.

The settings for peer-to-peer downloading are as follows:

Allow Symantec Management Agents to download packages from peer computers	<p>Enables the peer-to-peer downloading functionality that allows the client computers to download packages from their peers.</p> <p>Note that only the peer computers that are managed by the same Notification Server can download packages from each other.</p>
TCP/UDP port	<p>HTTP server listens to the TCP port. Peer discovery engine listens to the UDP port. The same port number is used for both.</p>
HTTP request timeout	<p>The period that the HTTP server should wait for the peer commands or file download requests from peer computers to arrive. If the request is not completed in a specified time, it is canceled with a timeout error.</p> <p>Note that if the timeout period is short (5-10 seconds), the slower client computers may drop out of the DHT network.</p>
Maximum upload bandwidth	<p>The maximum upload speed that the uploading peer can share between downloading peers.</p>
Maximum download bandwidth	<p>The maximum download speed that the Symantec Management Agent can use when downloading a package from a peer computer.</p> <p>Note that this value is independent from the general throttling value. For example, if you set the general throttling to 500 KB/s and peer-to-peer downloading throttling to 10 MB/s, the bandwidth is limited to 500 KB/s while downloading from Notification Server or Package Server outside the subnet, but the peer-to-peer downloading traffic inside the subnet has 10 MB/s bandwidth.</p>
Maximum number of requests per core	<p>The maximum number of simultaneous HTTP requests from the peer computers that the Symantec Management Agent's HTTP server processes. The rest of the requests are waiting.</p> <p>Note that this setting is per CPU core. For example, if you enter 5 for this option, the computers with dual core processor will have a total limit of 10 requests.</p>

Maximum number of connections	<p>The maximum number of simultaneous connections that the HTTP server allows.</p> <p>This option lets you limit the number of the client computers that can simultaneously connect to a peer.</p>
Total log size	<p>This option lets you control the total size of HTTP log files. The size of a single log file is 1 MB.</p>
Peer announcement	<p>A period after which Symantec Management Agent sends out a broadcast packet to its peers.</p>
Unavailable peer timeout	<p>A period after which a peer computer is considered as unavailable since it sends no broadcasts and does not answer to the requests.</p>
Build network for site	<p>This option forces the agent to create peer-to-peer network using only the subnets that belong to this agent's site(s).</p> <p>If your sites are organized in a way that the agents and subnets do not belong to multiple sites at the same time, this option can help you avoid cross-site downloads and manage package distribution at the site level.</p>
Build network for agent subnet(s)	<p>In peer-to-peer downloading, the Symantec Management Agent does not use any information of the subnet or site tree that you see in the Symantec Management Console. The agent only communicates to the peers that are available in the networks where computer's network adapters are connected to. The agent is not able to communicate to the computers located in the subnets that are not directly available.</p> <p>This option lets you configure additional network segments for peer engine to discover.</p> <p>Note that peers try to connect directly to the added subnets. Add the subnets only if the communication between the network segments is expected. If you expect communication only between very specific set of subnets, create a dedicated Targeted Agent Settings policy with additional subnets and target it correspondingly.</p>
Maximum number of peers per download attempt	<p>The maximum number of peers from which the Symantec Management Agent tries to download the package.</p> <p>Symantec suggests increasing this number if the computers often go offline.</p>

Maximum download attempts per package	<p>The maximum number of attempts to download a package using peer-to-peer downloading. Each attempt consists of selecting the specified number of peers and then attempting to download the package from each peer.</p> <p>If all the attempts fail, the Package Delivery will download the package directly from the Package Server or Notification Server.</p>
Period between download attempts	<p>The period of time after which the peer tries to download the package from another group of peers.</p> <p>Note that the timeout period for peer downloading does not increase. When a client computer downloads a package from Notification Server or Package Server, the timeout period increases on each attempt.</p>
File block download progress on peer	<p>This option lets you configure how often a peer computer notifies its peers about the package download progress. A peer computer downloads a file block by block. The size of each block is 2MB by default. The peer computer sends notifications about the package download progress after a specified period of time. If downloading of a file block is completed, other peers can start downloading it.</p>
Don't use peer-to-peer downloading	<p>In certain cases, you can disable using the peer-to-peer downloading.</p> <p>For example, if the computers are outside of the internal network and use Cloud-enabled Management for communicating with Notification Server.</p>

- 4 Click **Save changes**.

Configuring maintenance window policies

A maintenance window is a scheduled time and duration when maintenance operations may be performed on a managed computer. A maintenance operation is one that changes the state of a computer, causes it to restart, or interferes with a user's ability to operate the computer. For example, installing software and operating system patches, or running a virus scan.

A maintenance window policy defines one or more maintenance windows and is applied to a resource target in the same way as any other policy. These policies provide the maximum flexibility for assigning maintenance windows to computers, without complicating the management of agent settings. If multiple maintenance window policies apply to a single computer, changes to the computer are permitted during any of the maintenance windows.

Using maintenance windows lets you schedule maintenance work on managed computers with minimal effect on workflow and productivity. Also, you can schedule maintenance work on critical servers at different times so no two servers are ever restarted at the same time. A

maintenance window may be scheduled for certain times, such as daily, weekly or monthly. The maintenance window may be available indefinitely or restricted to a particular date range.

After you apply a maintenance window to a managed computer, you can configure the maintenance tasks, such as patches or software deliveries, to only run during the maintenance window.

The Symantec Management Agent processes the policy and provides the functionality that solutions use to determine whether a maintenance window is currently open. Functionality is also provided to allow solutions to inform Notification Server that a maintenance task has been performed.

If the Symantec Management Agent is performing a task as part of a job when the maintenance window expires, the maintenance window is automatically extended until all tasks that are contained in the job are completed.

You can create and modify the maintenance window policies that you need and apply them to the appropriate targets. The default maintenance window policy is applied to all managed computers.

To configure maintenance window policies

- 1 In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Maintenance Windows**.
- 2 In the left pane, do one of the following:
 - To create a new maintenance window policy, right-click the **Maintenance Windows** folder, and then click **New > Maintenance Window**.
 - To modify an existing maintenance window policy, click the appropriate policy.

3 In the right pane, in the **Time zone** drop-down list, click the appropriate option:

- | | |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use agent time | The times are specified without time zone information and are applied at the local time at each managed computer. Maintenance windows open and close at different times depending on the time zones of the managed computers. |
| Use server time | The times are specified with time zone information, where the time zone offset is that of the server's time zone where the policy is defined. The maintenance windows open simultaneously irrespective of time zones and are compensated for daylight saving.

This option ensures that maintenance windows are always coordinated with the specified local time on the server where the policy is created. |
| Coordinate using UTC | The times are specified with time zone information, where the time zone offset is 0. The maintenance windows open simultaneously irrespective of time zones and are not affected by daylight saving. |

The time zone applies to all of the maintenance windows that are specified in this policy.

4 If you want the policy to take effect on a particular date, rather than as soon as it is enabled, in the upper right corner, click **Advanced**, then in the **Advanced Options** dialog box, set the start date and end date, and click **OK**.

- | | |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start | The date that the policy takes effect. The policy must be enabled in the same way as any other policy. You can enable the policy at any time before or after the start date. |
| End | If you want the policy to be available for a limited period of time, set the appropriate end date. The policy is unavailable after this date, whether or not it is enabled.

This setting is optional. If no end date is specified, the policy is available indefinitely. |

5 To create the maintenance windows that you want to include in the policy, click **Add Maintenance Window**.

6 In each maintenance window, do the following:

- Under **Daily Times**, specify the start time of the maintenance window and either the end time or the duration in the corresponding boxes.
Alternatively, you can drag the green (start time) and red (end time) arrows to the appropriate places on the time line.
- Under **Repeat Schedule**, in the **Repeat every** drop-down list, select a schedule and then specify the appropriate schedule filters.

- 7 Under **Applied to**, specify the maintenance window policy target.

You can select an existing organizational group, filter, or resource target. You can also select individual resources.

Details of the selected items are displayed in the grid. You can view the list by targets, resources, computers, or users, and make any necessary additions and deletions.

- 8 Click **Save changes**.

See [“Configuring the Symantec Management Agent using the configuration policies”](#) on page 235.

Configuring a Notification Server communication profile

The communication profiles feature gives you an overview of the connections that the Symantec Management Agents use to communicate with Notification Servers or site servers. Communication profile defines the information that the Symantec Management Agents require to establish connection to Notification Server or site server.

Communication profile also lets you redirect the Symantec Management Agent to communicate with another Notification Server.

See [“Redirecting the Symantec Management Agent to communicate with a different Notification Server”](#) on page 248.

The default communication profile is created during the installation of Symantec Management Platform. You can additionally create or import communication profiles.

After you create the communication profile, you can right-click its name in the left pane and then click **Create Installation Package** to create an installation package for installing the Symantec Management Agent with the settings of this communication profile.

Alternatively, you can run `aexnsagent` command with the following options to apply the communication profile to the client computers:

- `/importprofile:<path>` - lets you specify the path to the XML file of the profile
- `/profilepwd:<pwd>` - lets you specify the decryption password

To configure a communication profile

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, under **Settings**, expand **Agents/Plug-ins > Symantec Management Agent**, right-click **Symantec Management Agent Communication Profiles**, and then click **New Profile**.
- 3 On the communication profile page, make the necessary changes.

For more information, click the page and then press **F1**.

Redirecting the Symantec Management Agent to communicate with a different Notification Server

- 4 Enable the settings.

At the upper right of the page, click the colored circle, and then click **On**.

- 5 Click **Save changes**.

Redirecting the Symantec Management Agent to communicate with a different Notification Server

(Windows only)

Communication profile defines the information that the Symantec Management Agents require to establish connection to Notification Server or site server.

See [“Configuring a Notification Server communication profile”](#) on page 247.

If you need to redirect some of the Symantec Management Agents to communicate with another Notification Server, you use the communication profile to perform this task.

To redirect the agents, you must first export the communication profile of the Notification Server computer to which you want to redirect the agents. The exported communication profile is an XML file that you can then import as follows:

Import the communication profile to the Notification Server that the agents currently use.

After you import the communication profile, you use the **Targeted Agent Settings** policy to apply this communication profile to the agents that you want to redirect.

Import the communication profile directly to the client computer.

You can import the communication profile directly to a client computer when the client computer has problems connecting to Notification Server or site server.

Note that you can only import the communication profile when you have enabled the diagnostics mode in the Symantec Management Agent.

To redirect the Symantec Management Agent to communicate with a different Notification Server

- 1 Open the Symantec Management Console of the Notification Server computer to which you want to redirect the Symantec Management Agents.
- 2 In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Symantec Management Agent**.

Redirecting the Symantec Management Agent to communicate with a different Notification Server

- 3 In the left pane, expand **Symantec Management Agent Communication profiles**, right-click the communication profile that you want to export, and then click **Export**.

Note that if Cloud-enabled Management is enabled on Notification Server from which you export the communication profile, the Cloud-enabled Management settings are also available for export. The exported Cloud-enabled Management settings let you switch the agents to that Notification Server in Cloud-enabled Management mode.

- 4 In the **Export SMP Server Communication Profile** dialog box, select the output format of the communication profile, specify the encryption password, and then click **OK**.

The output formats of the communication profile can be as follows:

Legacy encryption format Lets you store the communication profile in a format that is compatible with Symantec Management Platform 7.6.

FIPS compliant format Lets you store the communication profile in FIPS compliant format. This communication profile can be imported to Symantec Management Platform 8.0 and later.

- 5 In the **Save As** dialog box, specify the location to save the file, and then click **Save**.

- 6 To import the communication profile, do one the following:

To import the communication profile to the Notification Server that the agents currently use.

- 1 Open the Symantec Management Console of the Notification Server computer that the Symantec Management Agents currently use.
- 2 In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Symantec Management Agent**.
- 3 In the left pane, right-click **Symantec Agent Communication profiles**, and then click **Import profile**.
- 4 In the **Import Item** dialog box, specify the location of the communication profile file, enter the encryption password, and then click **OK**.
- 5 Use the **Targeted Agent Settings** policy to apply the communication profile to the Symantec Management Agents that you want to redirect.

On the **Targeted Agent Settings** policy page, on the **Advanced** tab, specify the communication profile that you imported.

Redirecting the Symantec Management Agent to communicate with a different Notification Server

To import the communication profile directly to the client computer.

- 1 On the client computer to which you want to import the communication profile, open the Symantec Management Agent UI and enable the **Diagnostics** mode.

Note that you must be logged on as an administrator to enable the **Diagnostics** mode.

See [“Enabling the Diagnostics mode in Symantec Management Agent”](#) on page 202.

- 2 On the **Agent Settings** tab, in the left pane, click **Import Profile**.
- 3 In the **Import Connection Profile** dialog box, select the communication profile, enter the encryption password, and then click **Import**.

Implementing Cloud-enabled Management

- [Chapter 20. Introducing Cloud-enabled Management](#)
- [Chapter 21. Preparing your environment for Cloud-enabled Management](#)
- [Chapter 22. Setting up Cloud-enabled Management](#)
- [Chapter 23. Performing Cloud-enabled Management tasks](#)

Introducing Cloud-enabled Management

This chapter includes the following topics:

- [About Cloud-enabled Management](#)

About Cloud-enabled Management

Cloud-enabled Management lets you manage client computers over the Internet even if they are outside of the corporate environment and cannot access the management servers directly. The managed computers do not need to use a VPN connection to your organization's network.

You can apply Cloud-enabled Management in the following scenarios:

- An organization with many employees traveling or working outside the office (outside the corporate intranet).
- A managed service provider (MSP) managing external companies.
- Highly distributed companies with many small offices or employees working from home.

When you implement Cloud-enabled Management, the Notification Server computer and site servers are not directly exposed to the Internet. Therefore, Symantec Management Agent communicates with the Notification Server computer and the site servers through an Internet gateway. Usually, two or more Internet gateways should be available to maintain reliable management of cloud-enabled client computers and to provide failover options. Each Internet gateway can support routing to multiple independent Notification Servers.

To use cloud-enabled management, you must install an Internet gateway server. The Internet gateway works as a tunneling proxy. It ensures the privacy and safety of the data that is passed between an agent and a management server with HTTPS communications. The Internet gateway is located in a demilitarized zone (DMZ) between two firewalls. It accepts incoming connections from authorized client computers on the Internet and forwards them to the

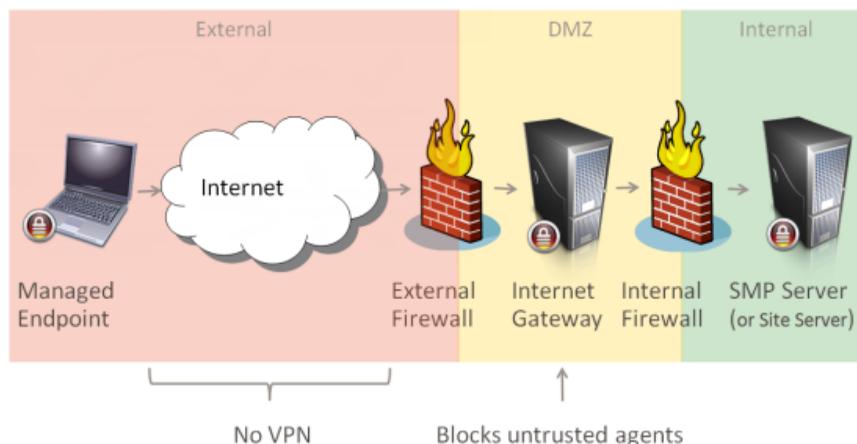
appropriate Notification Servers and site servers inside your network. The Internet gateway blocks any connection attempts by unauthorized client computers.

The Symantec Management Agent automatically determines whether routing the communication through the Internet gateway is needed or not. If a cloud-enabled computer has direct access to the local network using VPN, the agent automatically switches to a direct communication with Notification Server. If a cloud-enabled computer is outside the corporate network, the agent routes all communication on the Internet to Notification Server through the Internet gateway.

Note: Cloud-enabled Management is supported on Microsoft Windows computers and Mac OS X computers.

Not all solutions in IT Management Suite support Cloud-enabled Management. For more information on Cloud-enabled Management support for a particular solution, refer to the solution documentation.

Figure 20-1 Cloud-enabled Management



To use the Cloud-enabled Management feature, you do the following:

- Set up the infrastructure and configure your servers and client computers to use SSL. See [“Preparing your environment for Cloud-enabled Management”](#) on page 254.
- Install and configure the Internet gateways, configure the Cloud-enabled Management policies, and set up the Symantec Management Agents to support the Cloud-enabled Management environment. See [“Setting up Cloud-enabled Management”](#) on page 256.
- (Optional) Perform troubleshooting and maintenance tasks. See [“Cloud-enabled Management troubleshooting and maintenance tasks”](#) on page 272.

Preparing your environment for Cloud-enabled Management

This chapter includes the following topics:

- [Preparing your environment for Cloud-enabled Management](#)

Preparing your environment for Cloud-enabled Management

Configuring your environment to use SSL is a prerequisite for setting up Cloud-enabled Management (CEM). After you configure your environment to use SSL, you can set up Cloud-enabled Management.

See [“Setting up Cloud-enabled Management”](#) on page 256.

Table 21-1 Process for preparing your environment for Cloud-enabled Management

Step	Action	Description
Step 1	Configure your Notification Server computer and Symantec Management Agents to use HTTPS.	<p>Make sure that your Notification Servers are configured for HTTPS access.</p> <p>Note that Notification Server is automatically configured to use HTTPS if you check Require HTTPS to access the Management Platform on the Notification Server Configuration page, in Symantec Installation Manager, during the installation of IT Management Suite.</p> <p>If the Notification Server computer allows both HTTP and HTTPS connection, the Symantec Management Agents are automatically configured to use HTTPS when they receive the Cloud-enabled Management Settings policy.</p>
Step 2	Configure site servers to use HTTPS.	<p>To serve cloud-enabled agents, the site servers have to be configured to use HTTPS. This process is automated by the Global Site Server Settings. When a new site server is assigned to an Internet site, the CEM certificate is distributed and HTTPS binding is created on the port that is given in the settings.</p> <p>See “Configuring global site server settings” on page 109.</p> <p>You can also distribute a CEM certificate with individual installation settings to each site server separately.</p> <p>See “Configuring individual connection settings for a site server” on page 110.</p>

Setting up Cloud-enabled Management

This chapter includes the following topics:

- [Setting up Cloud-enabled Management](#)

Setting up Cloud-enabled Management

Before using Cloud-enabled Management, you must install and configure the Internet gateways. After that you must configure the Cloud-enabled Management policies and set up the Symantec Management Agents to support the Cloud-enabled Management environment.

Table 22-1 Process for setting up Cloud-enabled Management

Step	Action	Description
Step 1	Configure the Cloud-enabled Management Agent IIS Website Settings .	<p>A separate agent site on Notification Server is required for cloud-enabled agents. This site contains only agent interfaces and does not provide access to any of the Symantec Management Console pages. It also performs additional certificate and resource access checks to enforce security measures for agents connecting from the Internet.</p> <p>You must configure the Internet gateway to allow access only to cloud-enabled agent site on Notification Server.</p> <p>See “Configuring the Cloud-enabled Management Agent IIS Website Settings” on page 258.</p>

Table 22-1 Process for setting up Cloud-enabled Management (*continued*)

Step	Action	Description
Step 2	Prepare the Internet gateway computer.	<p>The Internet gateway computer should be located in your organization's demilitarized zone (DMZ) to ensure that it is protected from both the external and the internal networks.</p> <p>You need to configure the firewall on the gateway computer to allow incoming connections from the Internet only to the appropriate gateway port. After the configuration, the port opens automatically. You also need to configure the firewall to allow outgoing connections only to specific servers on your internal network.</p> <p>See "About preparing the Internet gateway computer" on page 260.</p>
Step 3	Download and run the Internet gateway installation package.	<p>To install the Internet gateway, you need to download and run the Internet gateway installation package from the Symantec Management Console.</p> <p>See "Downloading and running the Internet gateway installation package" on page 261.</p>
Step 4	Configure the Internet gateway using the Symantec Management Platform Internet Gateway Configuration wizard and the Symantec Management Platform Internet Gateway Manager .	<p>In the Symantec Management Platform Internet Gateway Configuration wizard, you specify the port for incoming connections, the SSL certificate information, and the user account.</p> <p>In Symantec Management Platform Internet Gateway Manager, add your Notification Server and your site servers to the list of servers that can communicate with the Internet gateway.</p> <p>You also need to copy the Gateway Certificate Thumbprint that you use for configuring the Cloud-enabled Management Settings policy. Note that if you enable the Internet gateway reporting, the thumbprint is automatically sent to Cloud-enabled Management Settings policy.</p> <p>See "Configuring the Internet gateway" on page 262.</p>
Step 5	Enable the Internet gateway status reporting.	<p>When Internet gateway reporting is turned on, the status information is sent cyclically to Notification Server.</p> <p>See "Enabling the Internet gateway status reporting" on page 264.</p>

Table 22-1 Process for setting up Cloud-enabled Management (*continued*)

Step	Action	Description
Step 6	Assign site servers to Internet sites.	<p>The cloud-enabled agents that are behind the Internet gateway use Internet sites for determining the site services.</p> <p>In the Symantec Management Console, you must add your site servers to a predefined Default Internet Site or other Internet sites that you create.</p> <p>See “Configuring sites and site servers to serve cloud-enabled agents” on page 265.</p>
Step 7	Make sure that the Internet site is properly configured.	<p>On the Internet site page, make sure that the required site services are set up properly and that the settings apply to the appropriate resource target.</p> <p>You can access the Internet site page in the Symantec Management Console, on the Site Server Settings page, under Site Management > Internet Sites.</p>
Step 8	Configure the Cloud-enabled Management Settings policy.	<p>The Cloud-enabled Management Settings policy lets you target the computers that you want to manage over the Internet. The policy also contains the list of Internet gateways that are available for the targeted client computers to use.</p> <p>See “Configuring the Cloud-enabled Management Settings policy” on page 267.</p>
Step 9	Install the Symantec Management Agent on the computers that cannot directly connect to the internal network.	<p>In some cases a computer that you want to manage may not have direct access to the network that hosts the Symantec Management Platform. To install the Symantec Management Agent on a computer that is located outside of the internal network, you must download the agent installation package from your Symantec Management Console, save it to suitable media, and then install it on the appropriate computers.</p> <p>See “Generating and installing the Cloud-enabled Management offline package” on page 269.</p>

Configuring the Cloud-enabled Management Agent IIS Website Settings

A separate agent site on Notification Server is required for cloud-enabled agents. This site contains only agent interfaces and does not provide access to any of the Symantec Management Console pages. It also performs additional certificate and resource access checks to enforce security measures for agents connecting from the Internet.

The Cloud-enabled Management Agent IIS site requires a connection that is secured with an SSL certificate. You can either import a commercial certificate or you can create a self-signed certificate.

This task is a step in the process for setting up Cloud-enabled Management.

See [“Setting up Cloud-enabled Management”](#) on page 256.

To configure the Cloud-enabled Management Agent IIS Website Settings

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Cloud-enabled Management**.
- 2 In the left pane, expand the **Setup** folder, and then click **Cloud-enabled Management Agent IIS Website Settings**.
- 3 On the **Cloud-enabled Management Agent IIS Website Settings** page, check **Add IIS Website for cloud-enabled management agent connections**, and specify the following settings:

Name	Lets you specify the name under which the website is displayed in the Internet Information Services (IIS) Manager .
Port	Lets you specify the port on which the website will be available. To set up Cloud-enabled Management, it is required that the selected port is reachable by the Internet gateway computer.
FQDN	Lets you see the actual FQDN of the Notification Server computer. You can specify an alternate FQDN here. This FQDN is placed in certificate along with all other FQDN-s that are detected for Notification Server.
Certificate	Lets you import a commercial certificate or create a self-signed SSL certificate.

Note: **Name** and **FQDN** cannot be changed after the **Cloud-enabled Management Agent IIS Website** is created.

- 4 Click **Save changes**.

Note: A package refresh task is part of the website creation process. In environments with large number of tasks it can take considerable amount of time. You can safely close Symantec Management Console once the following messages are logged:

```
Agent site creation task {Task_Guid} started.
```

```
Starting Package Refresh for all the packages.
```

About preparing the Internet gateway computer

The Internet gateway lets Symantec Management Agents on the Internet communicate with the Symantec Management Platform. The Internet gateway forwards requests from authenticated Symantec Management Agents to specific port numbers on Notification Server instances or site servers behind the gateway. By default, all requests are forwarded from the default HTTPS port 443 on the gateway to port 4726 on the Notification Server computer.

The Internet gateway creates a virtual tunnel through the internal firewall. It lets the authorized client computers on the Internet access the appropriate internal servers, but it keeps out all unauthorized client computers. The cloud-enabled Symantec Management Agent communicates with the Internet gateway directly, through the Internet. No VPN is required. When a cloud-enabled agent connects to it, the gateway and the agent exchange and verify each other's certificates. The gateway checks that the certificate was issued by a known Notification Server. The gateway then creates a tunnel that the agent can use to communicate directly to the appropriate Notification Server and site servers using HTTPS. When the agent has finished communicating with the target server, the tunnel connection is closed.

The Cloud-enabled Management feature does not support the use of proxy servers. You cannot set up a proxy between a Cloud-enabled Symantec Management Agent and the Internet gateway.

Symantec recommends that you configure at least two Internet gateways to provide failover options, load balancing, and to maintain communication continuity. Each Internet gateway can serve multiple Notification Servers. This configuration is supported even if Notification Servers are organized in a hierarchy.

Each Internet gateway supports 1- 35,000 endpoints and up to 20,000 concurrent connections.

The following examples help you decide how many Internet gateways you need in your environment:

- When you have 20,000 client computers on one Notification Server and 30% of them are cloud-enabled, the best practice is to have two Internet gateways to ensure high availability. However, even one Internet gateway can easily handle this configuration.
- If you have 180,000 client computers split across 2 hierarchies with 70% of them cloud-enabled, you need to have at least four Internet gateways: three to handle the node load and one for fault-tolerance.

Before you install the Internet gateway, you need to configure the host computer. The gateway computer should be located in your organization's demilitarized zone (DMZ) to ensure that it is protected from both the external and the internal networks. You need to configure the firewall on the Internet gateway computer to allow incoming connections from the Internet only to the appropriate gateway ports. You also need to configure the firewall to allow outgoing connections only to specific servers on your internal network.

If the gateway runs on a VMware virtual machine, you should use the VMXNET 3 network adapter. Note that VMXNET 3 is available only when you have VMware Tools installed on

your virtual machine. For more information about the VMXNET 3 network adapter, see the following VMware Knowledge Base article: [KB1001805](#).

Note: The Internet gateway computer must have Windows Server 2008 R2 SP1, Windows Server 2012 R2, or Windows Server 2016 (including Core Edition) operating system with the .NET Framework 4.5.1 or above enabled.

Symantec Management Platform does not need to manage the gateway computer. The Internet gateway is typically unmanaged.

Before you begin installation, verify that the Internet gateway computer can access the Notification Server computer and any required site server computers. When you verify the connection, use the host names or the IP addresses that the cloud-enabled agents attempt to connect to.

This task is a step in the process for setting up Cloud-enabled Management.

See “[Setting up Cloud-enabled Management](#)” on page 256.

Downloading and running the Internet gateway installation package

If you want to install or upgrade an Internet gateway, you first need to obtain the appropriate Internet gateway installation package. The installation package is an .EXE file that you can download from the Symantec Management Console. The package contains an installation wizard that guides you through the installation process.

Note: The installation package is also used to upgrade the Internet gateway.

If you can access the Symantec Management Console remotely from the Internet gateway computer, you can choose to run the Internet gateway installation package directly. Alternatively, you can save the file on any other media, copy it to the appropriate Internet gateway computer, and then run it.

Warning: Exit all Windows programs before you run the Internet gateway installation package.

This task is a step in the process for setting up Cloud-enabled Management.

See “[Setting up Cloud-enabled Management](#)” on page 256.

To download and run the Internet gateway installation package

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Cloud-enabled Management**.
- 2 In the left pane, expand **Setup**, and then click **Cloud-enabled Management Setup**.

- 3 On the **Cloud-enabled Management Setup** page, on the **Internet Gateway Setup** tab, click **Download the Internet gateway installation package**.
- 4 If you are on the gateway computer, you can click **Run** to run the installer immediately. If you want to save the package as a file to run later or to run on a different computer, click **Save**, specify the appropriate folder, and then click **OK**.
- 5 Navigate to the SMP Internet gateway installation package that you downloaded, and double-click `SMP_Internet_Gateway`.
- 6 In the **Open File - Security Warning** dialog box, click **Run**.
- 7 In the **Symantec Management Platform Internet Gateway Setup** dialog box, click **Next**.
- 8 Click **I accept the licence agreement**, and then click **Next**.
- 9 Specify the path to the destination folder where you want to install the Internet gateway files, click **Next**, and then click **Next**.
- 10 Make sure that **Start configuration wizard** box is checked, and then click **Finish**.

Configuring the Internet gateway

After the Internet gateway is successfully installed, you must configure it to work together with the Symantec Management Platform. You configure the Internet gateway using the **Symantec Management Platform Internet Gateway Configuration** wizard and the **Symantec Management Platform Internet Gateway Manager**.

In the **Symantec Management Platform Internet Gateway Configuration** wizard, you specify the port for incoming connections, the SSL certificate information, and the user account.

In **Symantec Management Platform Internet Gateway Manager**, you add your Notification Server and your site servers to the list of servers that can communicate with the Internet gateway. You also obtain the **Gateway Certificate Thumbprint** that you need for configuring the **Cloud-enabled Management Settings** policy.

This task is a step in the process for setting up Cloud-enabled Management.

See [“Setting up Cloud-enabled Management”](#) on page 256.

To configure the Internet gateway using the Symantec Management Platform Internet Gateway Configuration wizard

- 1 On the Internet gateway computer, in the **Symantec Management Platform Internet Gateway Configuration** wizard, on the **IP addresses and Ports** page, specify the appropriate IP address and ports, and then click **Next**.

By default, the port for incoming connections is 443. However, you can specify a different port number if necessary. All of the specified port numbers must be TCP ports (these are numbered 1-65535).

You should use the IP address of the Internet gateway computer. You can specify only one port number and only one IP address. If you choose to use all available IP addresses, the same port number is used for all IP addresses. If you require more granular control of IP addresses and port numbers, you need to edit the Apache configuration file directly.
- 2 On the **SSL FIPS** page, check the **Enable FIPS mode** box if you want to enable FIPS mode on your Internet gateway, and then click **Next**.
- 3 On the **SSL Certificate Information** page, specify the appropriate certificate information, and then click **Next**.

The Internet gateway must have an SSL certificate available so that Symantec Management Agents can communicate with it. The configuration wizard generates a self-signed SSL certificate based on the information that you provide.
- 4 On the **User Account** page, specify the appropriate user account information and then click **Next**.

Normally, you can use the **LocalService** account to set up the Internet gateway service. However, you can also use a dedicated user account if it is required for security reasons.
- 5 On the **Summary** page, review your setup, and then click **Finish**.

To configure the Internet gateway in the Symantec Management Platform Internet Gateway Manager

- 1 To open the **Symantec Management Platform Internet Gateway Manager**, click **Start > Programs > Symantec > Symantec Internet Gateway Manager**.

Note that after the **Symantec Management Platform Internet Gateway Configuration** wizard finishes, the **Symantec Management Platform Internet Gateway Manager** opens automatically.
- 2 To add your site servers and Notification Servers to the list of servers that can communicate with the Internet gateway, do the following:
 - In the **Symantec Management Platform Internet Gateway Manager**, on the **Servers** tab, click **Add Server**.

- In the **Add Server** dialog box, select if you want to add Notification Server or site server, add FQDN or host name of the server, edit the SSL port number if necessary and then click **OK**.
Note that the **Port** of the Notification Server computer must be the same as the one that you specify on the **Cloud-enabled Management Agent IIS Website Settings** page, in the Symantec Management Console.
 - If the **Certificate Warning** dialog box appears, click **Ignore**.
 - In the **Restart Service?** dialog box, click **Yes**.
- 3 To copy the **Thumbprint** that you need for configuring the **Cloud-enabled Management Settings** policy in the Symantec Management Console, on the **General** tab of the **Symantec Management Platform Internet Gateway Manager**, right-click the **Thumbprint**, and then click **Copy**.

See [“Configuring the Cloud-enabled Management Settings policy”](#) on page 267.

See [“Internet gateway management scripts”](#) on page 447.

Enabling the Internet gateway status reporting

Internet gateway provides a reporting capability. When Internet gateway reporting is turned on, the status information is sent cyclically to Notification Server.

This task is a step in the process of setting up Cloud-enabled Management.

See [“Setting up Cloud-enabled Management”](#) on page 256.

To enable Internet gateway status reporting

- 1 On the Internet gateway computer, start the **Symantec Management Platform Internet Gateway Manager**.
- 2 In the **Symantec Management Platform Internet Gateway Manager**, on the **Servers** tab, for the Notification Server that you want the Internet gateway to report the status to, enable the **Status report** option in the **Add Server** dialog box.
- 3 (Optional) In the **Symantec Management Platform Internet Gateway Manager**, on the **Settings** tab, under **Server's settings**, click the value to change the **StatusReportInterval**.

To view the reports that are generated from Internet gateway status reporting, in the Symantec Management Console, on the **Reports** menu, click **Reports > Notification Server Management > Cloud-enabled Management > Gateway**.

See [“Viewing Cloud-enabled Management reports”](#) on page 284.

Configuring sites and site servers to serve cloud-enabled agents

The computers that you want to manage over the Internet should be organized into one or more sites. These sites should be dedicated to cloud-enabled agents and must not contain any directly managed agents. Note that the Symantec Management Platform provides you with a predefined **Default Internet Site** with the **All Computers where the Cloud-enabled Management feature is enabled** target. You should then assign the appropriate site servers to the predefined site or to the sites that you create.

Note: Each internet site must have at least one site server assigned to it.

Cloud-enabled Management supports Internet package servers and Internet task servers, which the Symantec Management Agent accesses through an Internet gateway. Cloud-enabled Management also supports cloud-enabled package servers, which are the package servers located in the same site as the cloud-enabled agents. Only the local agents can access a cloud-enabled package server, and they use a direct connection. However, cloud-enabled task servers are not supported.

Cloud-enabled computers must be manually assigned to sites that are based on resource targets. Cloud-enabled agents do not recognize site assignments based on IP addresses and subnets. Manual assignment ensures that each computer remains a member of the appropriate site regardless of where the computer is physically located.

See [“Managing sites”](#) on page 99.

You can manually assign a cloud-enabled agent to multiple sites or site servers. The site servers that are available to the agent are a union of all the site servers in the assigned sites.

You can configure your site server settings for cloud-enabled agents in the following ways:

Create and configure new sites.	You can create and configure as many sites as required to suit your environment setup. A cloud-enabled agent or package server that is assigned to multiple sites receives the union of all the site servers in the assigned sites.
Assign the cloud-enabled agents directly to the site servers.	You can assign a resource target directly to the site server to ensure that the target members are given access to that particular site server only. The assignment by site method makes all of the site servers that are members of the assigned site available to the targeted cloud-enabled agents.

See [“Preparing your environment for Cloud-enabled Management”](#) on page 254.

To configure an Internet site to serve the cloud-enabled agents

- 1 (Optional) In the Symantec Management Console, create a new site and assign the appropriate resource target to the site.

This resource target contains the cloud-enabled agents and package servers. You can reuse the same resource target that is applied to the **Cloud-enabled Management Settings** policy.

See “[Managing sites](#)” on page 99.

- 2 Assign the appropriate site servers to the site in one of the following ways:

To manually assign the site server to the site

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the left pane, expand **Site Management > Site Servers > your_site_server_name**, and then click **Internet Sites**.
- 3 In the right pane, under **Detailed Information**, click **New**.
- 4 In the **Select a Internet site** dialog box, click the Internet site to which you want to assign the site server, and then click **OK**.

To assign the subnet(s) of the local site servers to the site

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the left pane, click **Site Management > Subnets**.
- 3 In the right pane, select the appropriate subnet.
- 4 On the toolbar, click **Assign to site**.
- 5 In the **Select a site** window, select the site to which you want to assign the subnet.

Note: A local site server is the one that exists in the same disconnected site as the cloud-enabled agents that it serves.

This type of assignment requires the disconnected site to have a unique subnet that does not overlap with subnets of internal client computers, if any. This configuration is not common, so this approach is not generally recommended.

See “[Assigning a site server to a site manually](#)” on page 108.

To directly assign cloud-enabled agents to a site server

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the left pane, expand the site server that you want to modify, and then click **Manually Assigned Agents**.
- 3 In the right pane, click **New**, specify the resource target that contains the appropriate cloud-enabled agents, and then click **OK**.

Configuring the Cloud-enabled Management Settings policy

The **Cloud-enabled Management Settings** policy lets you target the computers that you want to manage over the Internet. The policy contains the list of Internet gateways that are available for the targeted client computers. To specify the available Internet gateways, enter the appropriate details of each gateway.

Normally, you need to configure only one **Cloud-enabled Management Settings** policy. You need multiple policies only if you want to have finer grained control over which Internet gateways serve which cloud-enabled computers or if you want to perform manual load-balancing.

To generate an agent installation package, you need to create or select a **Cloud-enabled Management Settings** policy and apply it to the appropriate target computers. The list of available Internet gateways for the selected policy is included in the agent installation package. This list allows the newly installed agent to start communicating with Notification Server immediately. The new cloud-enabled computer is automatically added to the resource target of the selected policy.

Note that a cloud-enabled computer automatically reverts to direct communication with the local Notification Server when direct network access is available. It also automatically changes back to cloud-enabled mode when the direct connection is no longer available. For example, a laptop computer that is normally used at remote locations may be used occasionally in the office and connected to the internal network.

While the **Cloud-enabled Management Settings** policy targets a computer, the computer continues to communicate using the appropriate Internet gateways. If the internal network is properly configured, all traffic between the agent, the Internet gateway, and Notification Server stays inside the internal network. If the **Cloud-enabled Management Settings** policy is disabled or no longer targets the computer, the computer uses the Internet gateway for communication until the direct connection becomes available. Then the computer reverts to direct communication with the local Notification Server.

This task is a step in the process for setting up Cloud-enabled Management.

See [“Setting up Cloud-enabled Management”](#) on page 256.

To configure the Cloud-enabled Management Settings policy

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Cloud-enabled Management**.
- 2 In the left pane, expand **Policy**, and then click **Cloud-enabled Management Settings**.
- 3 On the **Cloud-enabled Management Settings** page, configure the policy as follows:

Set up the list of Internet gateways that accept external agent traffic.

To add an Internet gateway, in the **Edit Gateway Server** dialog box, specify its parameters as follows:

- **Server**

The fully qualified domain name (FQDN) of the Internet gateway computer.

- **Port**

The port number that the Symantec Management Agent must use to connect to the Internet gateway. The default is port 443.

- **Thumbprint**

Paste the **Thumbprint** value that you have copied on the Internet gateway computer, in the **Symantec Management Platform Internet Gateway Manager**, on the **General** tab.

See "[Configuring the Internet gateway](#)" on page 262.

Specify the target computers to which the policy applies.

If you want to bring the existing Symantec Management Agents under Cloud-enabled Management, you need to add these computers to the policy. After the agent on a client computer receives the **Cloud-enabled Management Settings** policy, it connects to Notification Server and requests its unique client certificate. When the agent has received its certificate and has no direct connection to Notification Server, it attempts to connect through the available Internet gateways that were specified in the policy. After the agent has connected successfully, it switches from directly managed mode to CEM mode.

- 4 Turn on the policy.

At the upper right of the page, click the colored circle, and then click **On**.

- 5 Click **Save changes**.

After the Symantec Management Agent receives the policy, it is ready to use the Cloud-enabled Management feature. Until the client computer is connected to the internal network, the Cloud-enabled Management mode remains inactive. When you disconnect the client computer from the internal network, Symantec Management Agent can connect to Notification Server through the Internet gateway, and Cloud-enabled Management becomes active automatically.

You can check the status of the Cloud-enabled Management mode in the Symantec Management Agent of the client computer, on the **Symantec Management Agent Settings** tab, under **Network Status**.

Generating and installing the Cloud-enabled Management offline package

In some cases, a computer that you want to manage may not have direct access to the network that hosts the Symantec Management Platform. To install the Symantec Management Agent on a computer that is located outside of the internal network, you first need to download the agent installation package from the Symantec Management Console.

See [“Cloud-enabled agent installation package parameters”](#) on page 448.

After you generate the agent installation package from the appropriate Symantec Management Platform instance, you need to send it to the remote site. You can upload the package to a certain location or send it on a physical medium such as CD or flash drive. The users at the remote site then run the agent installation package to install the Symantec Management Agent on their computers. The newly installed Symantec Management Agent immediately connects to Notification Server through the appropriate Internet gateway. You can use the same installation package to install the Symantec Management Agent on all of the computers at a particular remote site.

This task is a step in the process for setting up Cloud-enabled Management.

See [“Setting up Cloud-enabled Management”](#) on page 256.

To generate and install Cloud-enabled Management offline package

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Cloud-enabled Management**.
- 2 In the left pane, expand **Setup**, and then click **Cloud-enabled Management Setup**.
- 3 On the **Cloud-enabled Management Setup** page, on the **Symantec Management Agent Configuration** tab, click **Generate and download Symantec Management Agent installation package**.

- 4 In the **Cloud-enabled Agent Installation Package** dialog box, specify the appropriate package parameters.

For more information, click the page and then press **F1**.

See [“Cloud-enabled agent installation package parameters”](#) on page 448.

- 5 Click **Generate Agent Installation Package**.

The package generation may take a few minutes. When the package is ready, you are prompted to run or save the file.

The generated installation package is a self-extracting agent installation package that includes the following components and settings:

- Symantec Management Agent installer for the appropriate platform.
- Notification Server address (including protocol and port number to use).
- Notification Server certificate with CA chain.
The Internet gateway certifies the thumbprint and the temporary certificate. The temporary certificate is used to connect to the gateway for the first time. The temporary certificate is essential as it is used to generate a permanent client certificate request.
- List of the Internet gateways that are available for the cloud-enabled agent to use.
- Organizational group to which the computer is added automatically.
(Windows only) Note that if you add multiple organizational groups, the end user must select the suitable organizational group on the client computer during the offline package installation.
- Scripts for configuring the Symantec Management Agent to use the specified settings.

Warning: The Symantec Management Agent installation package is valid for a limited time period (by default, 7 days) from the moment it was generated. The temporary certificate that is included in the package expires after this time. If you use the package after its temporary certificate has expired, the installed agent cannot use the Internet gateway for communications. You need to reinstall the agent using a newly generated installation package that contains a valid certificate.

- 6 In the **File Download** dialog box, click **Save**, and then specify the location to which to save the file.
- 7 When the package download is complete, click **Close**.
- 8 In the **Cloud-enabled Agent Installation Package** dialog box, click **Close**.
- 9 Place the Symantec Management Agent installation package on the appropriate computer.

- 10 Run the agent installation package on the computer.

Note: Windows agent package is a self-extracting executable file that requires a password to decrypt data and perform the installation. If the package contains information about more than one organizational group, the end user must also select the organizational group to which the computer belongs. Depending on the selected organizational group, appropriate communication profile with Cloud-enabled Management information is applied to the agent.

OS X package is a compressed file that contains **Symantec_Management_Agent_Installer.pkg** file to perform the interactive installation, a **Resource** folder with the actual signed agent packages, and **cem_package.sh** file to perform the silent installation using terminal.

After the installation, the Symantec Management Agent automatically configures itself, and then renegotiates its certificate.

The new certificate is specific to that client computer and replaces the temporary certificate that was included in the agent installation package. The agent requests and receives a new certificate from Notification Server:

See [“Cloud-enabled agent installation package for Mac computer”](#) on page 450.

- 11 Verify that the installation was successful. You can use the Symantec Management Console to view the reports to check that the newly managed computer is present.

If you specified an organizational group in the installation package, you can also check that the new computer has been added to the appropriate group.

See [“Viewing Cloud-enabled Management reports”](#) on page 284.

Performing Cloud-enabled Management tasks

This chapter includes the following topics:

- [Cloud-enabled Management troubleshooting and maintenance tasks](#)

Cloud-enabled Management troubleshooting and maintenance tasks

This section outlines the troubleshooting and maintenance tasks that you may need to perform.

See [“About Cloud-enabled Management”](#) on page 252.

Table 23-1 Cloud-enabled Management troubleshooting and maintenance tasks

Task	Description
Managing certificates.	The Manage Certificates page lets you check the certificates that are used in your environment and perform necessary management tasks. You can replace the certificates where necessary. You can revoke or renew agent certificates. See “Managing certificates” on page 273.
Applying a CEM certificate with individual installation settings to a site server.	You can distribute a CEM certificate with individual installation settings to each site server separately. See “Configuring individual connection settings for a site server” on page 110.
Restoring Cloud-enabled Management communication after an off-box upgrade.	After you perform an off-box upgrade of the IT Management Suite to the latest version, you may need to restore the communication with cloud-enabled client computers. See “Restoring Cloud-enabled Management communication after an off-box upgrade” on page 276.

Table 23-1 Cloud-enabled Management troubleshooting and maintenance tasks (*continued*)

Task	Description
Revoking a client certificate on a managed computer.	If you think a particular client certificate has been compromised and should no longer be trusted, you can revoke the certificate. For example, if a cloud-enabled laptop computer is lost or stolen you need to revoke its certificate immediately. Revoking the certificate prevents the managed computer from accessing your network in cloud-enabled mode. See "Revoking a Cloud-enabled Management certificate" on page 278.
Viewing site server certificates.	You can view site server certificates that are used in your environment. See "Viewing the site server certificates" on page 280.
Forcing a cloud-enabled agent to use a specified Internet gateway.	If the agent does not have a valid list of Internet gateways, you can force it to communicate through a specified set of gateways. You can add and remove Internet gateways from the list as required. Note: You can perform this task on Windows computers only. See "Forcing the Symantec Management Agent to use a specified Internet gateway" on page 281.
Backing up and restoring Internet gateway.	You can back up your Internet gateway settings and restore its original state in case of a failure. See "Backing up and restoring an Internet gateway" on page 282.
Configuring the load balancer to work with the Cloud-enabled Management traffic.	Cloud-enabled Management feature requires firewall to redirect all inbound CEM traffic directly to the Internet gateway. In a situation where all the inbound traffic (including CEM traffic) must be routed through the organization's load balancer, you must configure the load balancer to handle the Cloud-enabled Management traffic. The following knowledge base article explains, how to perform the configuration in F5 BIG-IP Local Traffic Manager . http://www.symantec.com/docs/HOWTO109667
Viewing Cloud-enabled Management reports.	A set of predefined reports is provided to help you monitor and manage your cloud-enabled computers. See "Viewing Cloud-enabled Management reports" on page 284.

Managing certificates

The **Certificate Management** page gives you a complete overview of the certificates that are used in your environment and lets you perform necessary management tasks.

Note: Note that information about the certificates is available immediately after the upgrade. However, before performing any certificate management tasks, you must upgrade the Symantec Management Agent to the latest version on all client computers. If you have implemented Cloud-enabled Management (CEM) in your environment, you must also upgrade the Internet gateway(s).

The **Certificate Management** page lets you check the state of the certificates. If a problem with a certificate is detected, the status of the certificate changes accordingly. For example, a certificate has a weak signature or its expiration date is near. In the list of certificates, you can filter out the certificates with detected problems and take required steps to fix the issues. Depending on the certificate type, you can replace, renew, or revoke selected certificates.

Note: Currently, the certificates that are manually added to the **Communication Profiles** are not displayed on the **Certificate Management** page.

To manage certificates

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Notification Server**, and then click **Certificate Management**.
- 3 On the **Certificate Management** page, you can do the following:

Replace certificate

To perform the replacement of certificate:

- 1 Click the certificate that you want to replace, and then, on the toolbar, click **Replace**.
- 2 Select the new certificate and confirm the replacement process.

Note that the replacement of the certificate does not occur immediately and the replacement process does not break the connectivity.

After you initiate the replacement, the certificate is distributed to the required computers. On the **Certificate Management** page, you can check the progress of certificate distribution.

- 3 When the distribution of certificate is completed, you can finalize the replacement.

Click the certificate that is being replaced, and then, on the toolbar, click **Finalize**.

The finalization task replaces the current certificate with a new one. After finalization, the new certificate will be in use.

If you have not enabled the **Auto Refresh...** option in the **Internet Gateway Manager**, on the **Servers** tab, take the following steps to perform the replacement of NS root certificate:

- 1 Initiate the replacement of NS root certificate.
- 2 On the Internet gateway computer, in the **Internet Gateway Manager**, on the **Servers** tab, manually refresh the required server.
- 3 Wait until the certificate is distributed to all client computers.
- 4 Finalize the replacement process.
- 5 On the Internet gateway computer, in the **Internet Gateway Manager**, on the **Servers** tab, manually refresh the required server.

Note that while the replacement is in progress, you can cancel it. Canceling the replacement process does not break connectivity and the old certificate remains in use.

Renew certificate

The renewal task lets you re-create CEM Agent certificates on cloud-enabled agents.

This task also lets you re-create an Internet gateway reporting certificate that the Internet gateway uses for sending its inventory to Notification Server.

To renew a certificate:

- ◆ Click the certificate that you want to renew, and then on the toolbar, click **Renew**.

If you have not enabled the **Auto Refresh...** option in the **Internet Gateway Manager**, on the **Servers** tab, take the following steps to perform the renewal of Internet gateway reporting certificate:

- 1 Initiate the renewal of Internet gateway reporting certificate.
- 2 On the Internet gateway computer, in the **Internet Gateway Manager**, on the **Servers** tab, manually refresh the required server.

Revoke certificate

Revoking a CEM Agent certificate prevents the managed computer from accessing your network in cloud-enabled mode. For example, if a cloud-enabled laptop computer is lost or stolen you need to revoke its certificate immediately.

To revoke a certificate:

- ◆ Click the certificate that you want to revoke, and then on the toolbar, click **Revoke**.

Restoring Cloud-enabled Management communication after an off-box upgrade

After you perform an off-box upgrade of the IT Management Suite 8.0 HF6 or 8.1 RU7 to the latest version, you may need to restore the communication with cloud-enabled client computers.

In most cases, when you upgrade the IT Management Suite onto a new server, the server has a different IP address and FQDN than the previous one. This means that the new server has a new set of SSL certificates that are used for Cloud-enabled Management (CEM) communication, and you need to set up CEM on the new Notification Server.

The following procedures describe the possible ways to redirect cloud-enabled clients after an off-box upgrade.

To restore CEM communication on Mac OS X computers that have no direct connection with Notification Server after an off-box upgrade of the IT Management Suite 8.0 HF6 or 8.1 RU7

- 1 After you install the latest version of IT Management Suite on the new server, configure CEM environment the same way, as for a new installation.

For more information on how to configure Cloud-enabled Management, see the *IT Management Suite Administration Guide*, or the *Cloud-enabled Management Whitepaper*.

- 2 On the new Notification Server, generate an offline installation package for CEM, extract `cem_package.sh` from the generated zip archive, and then place the package in a location accessible from old Notification Server.
- 3 On the old Notification Server, import the package into **Software Catalog**, and then set up the following `Install` command line option for the package:

```
sh cem_package.sh -reinstall -pwd 'yourpassword' -bg
```

This command line enables automated upgrade and switching to a new Notification Server.

- 4 From the old Notification Server, deploy the offline installation package to cloud-enabled clients with a **Managed Software Delivery** or a **Software Delivery task**.
- 5 When the clients are upgraded, on the new Notification Server, make sure that the newly upgraded clients are members of all needed filters and organizational groups.

To restore CEM communication on Mac OS X computers after an off-box upgrade of the IT Management Suite 8.0 HF6 or 8.1 RU7

- 1 Ensure that the 8.0 HF6 or 8.1 RU7 clients are able to communicate with the latest version of Notification Server without using CEM.
- 2 On the 8.0 HF6 or 8.1 RU7 Notification Server, disable the CEM policy to remove the old CEM settings from the clients.
- 3 In the **Symantec Management Console**, click **Settings > Agents/Plug-in Settings > Targeted Agents Settings**.
- 4 On the **Targeted Agents Settings** page, on the **Advanced** tab, redirect the clients to the latest version of Notification Server.
- 5 On the latest version of Notification Server, enable the CEM policy.

After the 8.0 HF6 or 8.1 RU7 clients register on the latest version of Notification Server and receive the CEM policy, they receive the new CEM settings.

To restore CEM communication on Windows or Mac OS X computers after an off-box upgrade of the IT Management Suite 8.0 HF6 or 8.1 RU7

- 1 After you install the latest version of IT Management Suite on the new server, configure CEM environment the same way, as for a new installation.
 For more information on how to configure Cloud-enabled Management, see the *IT Management Suite Administration Guide*, or the *Cloud-enabled Management Whitepaper*.
- 2 On the new Notification Server, export the default connection profile that includes CEM settings.
- 3 On the old Notification Server, import the connection profile.
- 4 In the **Symantec Management Console**, click **Settings > Agents/Plug-in Settings > Targeted Agents Settings**.
- 5 On the **Targeted Agents Settings** page, on the **Advanced** tab, check **Specify an alternate URL for the Symantec Management Agent to use to access the NS**, and then select and configure the imported connection profile.
- 6 Apply **Targeted Agent Settings** policy to the cloud-enabled clients that you want to upgrade, and then enable the policy.
- 7 Ensure that the targeted cloud-enabled clients receive the policy and use the imported connection profile to access Notification Server.
- 8 On the new Notification Server, enable the upgrade policy.
- 9 Ensure that the targeted cloud-enabled clients receive the policy and upgrade successfully.

Revoking a Cloud-enabled Management certificate

Revoking a Cloud-enabled Management (CEM) certificate prevents the managed computer from accessing your network in cloud-enabled mode. For example, if a cloud-enabled laptop computer is lost or stolen you need to revoke its certificate immediately.

The agent has two CEM certificates. One certificate lets the agent create connection to the Internet gateway, and another certificate lets the agent connect to Notification Server. If the certificate that lets the agent connect to Notification Server is revoked, Notification Server declines connection from such client computer. However, Internet gateway cannot receive the information on revoked certificates from Notification Server directly. To revoke a particular certificate on Internet gateway, you need to add the certificate details to the Certificate Revocation List (CRL) on Notification Server, generate an updated CRL file, and then apply the updated CRL file to the appropriate Internet gateway

Note: You need to apply the updated CRL file to every Internet gateway that the revoked agent might use.

Note that revocation of the cloud-enabled certificate only blocks the managed computer from accessing Notification Server in cloud-enabled mode. If the agent trust is not revoked, the agent can continue to operate in local mode.

To revoke a Cloud-enabled Management certificate

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, under **Reports**, expand **Notification Server Management > Certificates**, and then click **Certificate by Thumbprint**.
- 3 On the **Certificate by Thumbprint** report page, right-click the certificate that you want to revoke, and then click **Revoke Certificate**.

If you revoke the certificate on the **Certificate by Thumbprint** report page, the certificate details are added to the CRL file automatically.

The CRL is stored in the root computer store, although the certificates are stored in the Configuration Management Database (CMDB). The certificate revocation tool (`AeXRevokeCertificate.exe`) first loads the existing CRL if it exists. If no CRL exists in the certificate store, the tool creates one. The tool then adds the certificate serial number to the list and generates a PEM-encoded file containing the updated CRL. You then place the generated CRL file on the Internet gateway computer and run a script to apply the updated list to the Internet gateway.

By default, the CRL file is at the following location on Notification Server:

```
\Program Files\Altiris\Notification
Server\bin\Tools\AeXRevokeCertificate\EMEncodedFile.CRL
```

To add a Cloud-enabled Management certificate to the CRL manually

- 1 Obtain the serial number and thumbprint of the client certificate that you want to revoke.

If you have access to the client computer, you can use the Microsoft Management Console (MMC) to look up the client certificate details.

If you do not have access to the client computer, you can use one of the following methods:

- In the Symantec Management Console, open the Resource Manager and view basic inventory information for the client computer. The menu path is **View > Data Classes > Inventory > Basic Inventory > AeX AC Certificate**. The full details of the client certificate are shown, including the serial number and the thumbprint.
- Use a SQL query to search for the serial number and the thumbprint of the client certificate in the Symantec Management Platform CMDB, in the **CertificateRegistration** table.
- On the Internet gateway, open the access log file and look for an entry that relates to the client computer. The `access.log` file is stored in the `Apache\logs` folder in the Internet gateway installation folder. Each entry in the log file includes the name of the

computer that accessed the Internet gateway and the corresponding certificate serial number.

- 2 On the Notification Server computer, in the command prompt window, run the following command line with the appropriate parameters:

```
\Program Files\Altiris\Notification Server\bin\Tools\AeXRevokeCertificate
-o <PEMEncodedFile.CRL> <-t Sha256ThumbPrint | -s SerialNumber>
```

PEMEncodedFile.CRL The full path and name of the PEM-encoded CRL file that you want to generate. Without this parameter, the generated file is saved in the local directory.

Sha256ThumbPrint The unique identifier of the certificate.

SerialNumber If more than one certificate in the database is with the same serial number, use an SHA256 thumbprint to identify the certificate. If two certificates have the same thumbprint, identify the certificate by serial number.

Warning: Sometimes, the thumbprint and the serial number may be displayed as space-separated octets. However, when you specify them as command line parameters, they must not include any spaces between the characters.

The updated CRL file is generated.

To apply the CRL to an Internet gateway

- 1 Place the generated CRL at the following location on the Internet gateway computer:

```
[Internet gateway installation folder]\Apache\certs\crl
```

The default Internet gateway installation folder is `\Program Files x86\Symantec\SMP Internet Gateway`. However, the path depends on the target directory that was specified during the Internet gateway installation.

- 2 In the same folder, double-click **UpdateCrlHashes.cmd** to run the **Update CRL** script.

This script performs the necessary configuration, and then restarts the Internet gateway to apply the changes.

See [“Cloud-enabled Management troubleshooting and maintenance tasks”](#) on page 272.

Viewing the site server certificates

Under the **Organizational Views and Groups**, the **Digital Certificate** view displays the certificates that the site servers use. Note that the **Digital Certificate** view is disabled by default.

See [“Cloud-enabled Management troubleshooting and maintenance tasks”](#) on page 272.

To view the site server certificates

- 1 In the Symantec Management Console, on the **Manage** menu, click **Organizational Views and Groups**.
- 2 In the left pane, click **Default**.
- 3 In the right pane, on the upper right corner, click **Filter**.
- 4 In the **Filter Visible Groups** dialog box, under **Default > All Resources**, check **Digital Certificate** box, and then click **OK**.
- 5 In the left pane, expand **Default > All Resources**, and then click **Digital Certificate**.

Forcing the Symantec Management Agent to use a specified Internet gateway

(Windows agent only)

If the agent does not have a valid list of Internet gateways, you can force it to communicate through a specified set of gateways. You force a specific list of gateways from the command line or by modifying the registry settings. A command line is available for adding individual gateways.

To remove an Internet gateway from the Symantec Management Agent configuration, you need to edit the registry.

The Internet gateway details are stored in the registry. To add or remove Internet gateways, edit the entries under the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Communications\Secure Gateways
```

Each Internet gateway has a set of values under the <GatewayName> key.

Note: You need to restart the Symantec Management Agent to apply these settings.

To force the Symantec Management Agent to use a specified Internet gateway

- ◆ On the client computer, in the command prompt window, run the following command line:

```
\Program Files\Altiris\Altiris Agent\AeXNSAgent.exe  
/gw=gatewayName,port,thumbprint
```

gatewayName	The name or IP address of the gateway computer.
port	The port number that the Symantec Management Agent must use to connect to the gateway. The default port is 443.
thumbprint	The certificate thumbprint of the certificate that the gateway uses for secure connections. Warning: Sometimes, the thumbprint may be displayed as space-separated octets. However, when you specify it as a command line parameter, it must not include any spaces between the characters.

Each parameter needs to be separated with a comma. No spaces or other punctuation is allowed.

For example:

```
\Program Files\Altiris\Altiris Agent\AeXNSAgent.exe  
/gw=myGateWay.symantec.com,443,0f8753ef3da6bc4
```

See [“Cloud-enabled Management troubleshooting and maintenance tasks”](#) on page 272.

See [“Command line switches for Windows cloud-enabled agent configuration”](#) on page 451.

Backing up and restoring an Internet gateway

Backing up your Internet gateway lets you restore its original state in case of a failure. You can perform a partial restore if some files from the backup list are missing or corrupted. You can also perform a full restore in case of fatal corruptions in the Internet gateway configuration. For example, if you have replaced a hard disk on your Internet gateway computer.

You can perform a backup without stopping the Internet gateway service.

You can manually back up the files in given folders as follows:

- `openssl.cnf`, `server.crt`, and `server.key` files in the `C:\Program Files\Symantec\SMP Internet Gateway\Apache\certs` folder
- All files in the `C:\Program Files\Symantec\SMP Internet Gateway\Apache\certs\client` folder
- All files in the `C:\Program Files\Symantec\SMP Internet Gateway\Apache\certs\crl` folder

- All files in the `C:\Program Files\Symantec\SMP Internet Gateway\Apache\conf` folder

You can also create a backup file in the **Symantec Management Platform Internet Gateway Manager**.

To create a backup file

- 1 In the **Symantec Management Platform Internet Gateway Manager**, on the **Settings** tab, click **Save configuration to a file**.
- 2 In the **Save configuration** dialog box, enter the file name and password, and then click **OK**.

To perform a manual restore

- 1 On the Internet gateway computer, open the **Symantec Management Platform Internet Gateway Manager**.
- 2 On the **General** tab, under **Internet Gateway Service**, click **Stop** to stop the Internet gateway service.
- 3 Restore the required items from the backup list.
- 4 In the **Symantec Management Platform Internet Gateway Manager**, on the **General** tab, under **Internet Gateway Service**, click **Start** to start the Internet gateway service.

After you start the service, make sure that the Internet gateway settings are correct and the functionality is working properly.

To perform a full restore using the backup file

- 1 Perform a new installation of Internet gateway.
 See [“Downloading and running the Internet gateway installation package”](#) on page 261.
- 2 In the **Symantec Management Platform Internet Gateway Configuration** wizard, on the **First Time Setup** page, select **Use existing configuration**, and then click **Browse**.
- 3 In the **Restore Configuration** dialog box, select the configuration file, enter the password, and then click **OK**.
- 4 In the **Symantec Management Platform Internet Gateway Configuration** wizard, click **Next**.
- 5 On the **User Account** page, specify the Internet gateway service credentials, and then click **Next**.
- 6 On the **Summary** page, review the settings, and then click **Finish**.

After the service starts, make sure that the Internet gateway settings are correct and the functionality is working properly.

See [“Cloud-enabled Management troubleshooting and maintenance tasks”](#) on page 272.

Viewing Cloud-enabled Management reports

A set of reports is provided to help you monitor and manage your cloud-enabled computers. You can also create custom reports to suit your requirements.

See [“Creating and modifying custom Notification Server reports”](#) on page 378.

Cloud-enabled Management reports are grouped into the following folders:

Agent	The reports contain data about cloud-enabled computers.
Certificates	The reports contain data about SSL certificates, CEM offline installation packages, and their registration requests.
Gateway	The reports contain data about Internet gateways. See “Enabling the Internet gateway status reporting” on page 264.

To view Cloud-enabled Management reports

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, click **Reports > Notification Server Management > Agent > Cloud-enabled Management**, and then click **Agent**, **Certificates**, or **Gateway**.
- 3 Click the report that you want to view.

See [“Cloud-enabled Management troubleshooting and maintenance tasks”](#) on page 272.

Managing Symantec Management Platform resources

- [Chapter 24. Configuring resource security](#)
- [Chapter 25. Configuring resource filters and targets](#)
- [Chapter 26. Configuring packages](#)
- [Chapter 27. Using policies](#)
- [Chapter 28. Using tasks and jobs](#)
- [Chapter 29. Using Resource Manager](#)
- [Chapter 30. Using Notification Server reports](#)
- [Chapter 31. Creating custom Notification Server reports](#)
- [Chapter 32. Viewing resource information](#)
- [Chapter 33. About Symantec Remote Access Connector](#)
- [Chapter 34. Configuring Symantec Security Cloud Connector](#)

Configuring resource security

This chapter includes the following topics:

- [Configuring resource security](#)
- [Considerations for resource scoping](#)

Configuring resource security

The resource security model has changed significantly for Notification Server 7.0. Resources, which includes all computers, users, and everything else that is defined in the CMDB or resource model, now obtain all of their permission grants from the organizational views and groups to which they belong. This replaces the Notification Server 6.0 implementation, which required securing both standard collections and resource folders.

Note: There are a few exceptions, such as packages, which are resources but are also items that appear in the Symantec Management Console folder structure. The security options for these items are disabled in the folder structure. Security for these is set in the same way as other resources.

An organizational view is a hierarchical grouping of resources (as organizational groups) that reflects a real-world structure or view of your organization. For example, you may create organizational views to group your resources by geographical location, or by department, or by network structure. As in the real world, a resource may (but is not required to) appear once only in an organizational view.

The assignment of resources into organizational groups is automatic and you cannot change it. Note that there may be a delay between the resource being discovered and being shown in the appropriate organizational group. Each newly discovered resource is placed in the top

level organizational group, and remains there until being moved into the appropriate organizational group when the Organizational View refresh schedule runs.

You can remove resources from any organizational view except the **Default** view. When a resource is deleted from the CMDB, it is automatically removed from all organizational views using the delta update schedule.

See [“Scheduling resource membership updates”](#) on page 315.

You set up security by assigning the appropriate permissions for each security role on each organizational view, and on the organizational groups within each view. A permission that is assigned to an organizational group applies to all resources in that group and, by default, applies to all of its child groups. You cannot assign permissions directly to a particular resource.

Permission grants on a resource are accumulated across organizational views. The permissions that a security role has on a particular resource is the union of all the permissions that the resource has been assigned through the organizational groups to which it belongs. If a security role has permission to perform an action on a resource in one organizational view, the role can perform that action regardless of whether the permission is applied to other organizational views that contain the same resource. For example, if a security role has read access to a resource in one organizational view, write access to the same resource in another organizational view, but no access to the resource in a third organizational view, the role has both read and write access to the resource.

Implementing resource security in this way gives each security role its own unique view, or "scope", of the available resources. The security role determines which resources its members can access, and what actions they can perform on those resources. Filters, targets, and report results are dynamic and automatically scoped according to the role of the user who owns them. Therefore, filters, targets, and report results always contain only the resources to which that user has the necessary access permissions.

Configuring resource security is an optional step in the process of setting up Symantec Management Platform security.

See [“Setting up Symantec Management Platform security”](#) on page 62.

Note: When a target is evaluated, only resources to which the user has read access are available. Consequently, the only security permission that a user requires to apply a task or policy to a resource is the read permission on the resource.

Table 24-1 Process for configuring resource security

Step	Action	Description
Step 1	Identify your resource management and security requirements.	You need to determine your resource management and security requirements, and plan the organizational view structures that best meet your requirements. You can use any structure that you want. For example, you may want to use organizational views that are based on geography, business function, or management structure. For more information, see the <i>IT Management Suite Planning for Implementation Guide</i> .
Step 2	Create the organizational views that you want.	Create the organizational views that you need to model the appropriate logical structures in your organization. See “Creating and configuring an organizational view” on page 288. See “Creating and populating an organizational view or group” on page 289.
Step 3	Under each organizational view, create the organizational groups that you want and assign the appropriate resources to each organizational group.	Within each organizational view, you can create a hierarchy of groups to represent the organizational structure that you want to model. New resources are automatically added to the Default organizational view. You can move them to the appropriate groups within each of your organizational views. See “Creating and configuring an organizational group” on page 290. See “Viewing resources in an organizational group” on page 291.
Step 4	Assign the appropriate security roles to each organizational group.	Assigning a security role to an organizational group gives users with that role access to all resources that are directly included in that group. You need to specify the permissions that each role has on the group. By default, security settings on a group apply to all of its child groups. You can break the inheritance when necessary. See “Setting security on an organizational group” on page 292.

Creating and configuring an organizational view

An organizational view is a hierarchical grouping of resources (as organizational groups) that reflects a real-world structure or view of your organization. For example, you may create organizational views to group your resources by geographical location, or by department, or by network structure. As in the real world, a resource may (but is not required to) appear once only in an organizational view.

Organizational views provide a secure means of segregating your resources into well structured and manageable units. An organizational view cannot contain any resources directly - all resources must be contained in organizational groups. You can use organizational views and groups to model a wide variety of organizational requirements. You can secure your organizational views using the familiar NT security inheritance model that is used throughout the Symantec Management Platform.

You can use organizational views and groups within targets when you want to apply a policy or task to selected computers, users, or resources. The organizational view or group is used in the same way as a filter, but provides the security that is required to ensure that only the resources to which the target owner has permission are included.

This task is a step in the process for configuring resource security.

See [“Configuring resource security”](#) on page 286.

To create an organizational group

- 1 In the Symantec Management Console, on the **Manage** menu, click **Organizational Views and Groups**.
- 2 In the left pane, right-click the **Organizational Views** folder and then click **New > Organizational View**.
- 3 (Optional) In the right pane, edit the name and the description of the organizational view.
- 4 To specify the organizational groups that are displayed, do the following:
 - In the right pane, click **Filter**.
 - In the **Filter Visible Groups** dialog box, check the organizational groups that you want to be visible for this organizational view, and then click **OK**.

Creating and populating an organizational view or group

In the **Computers** Management view, you can create and populate organizational views and groups.

To create and populate an organizational view or group

- 1 In the Symantec Management Console, on the **Manage** menu, click **Computers**.
- 2 In the navigation pane, under **Computer Views and Groups**, right-click, and then click **New Organizational View**.
- 3 In the **Organizational View** dialog box, type the name for the organizational view, and then click **OK**.
- 4 Right-click the new organizational view, and then click **New > Organizational Group**.

Note that you cannot add organizational groups to the default **All computers** organizational view.

- 5 In the **Organizational Group** dialog box, type the name for the new group, and then click **OK**.
- 6 Under **Computer Views and Groups**, click **All Computers**, and then, in the content pane, select the computers that you want to add to this organizational group.
You can select multiple computers.
- 7 Right-click the selected computers, and then click **Add to organizational group**.
In the **Add to organizational group** dialog box, click the group that you want to add the computers to, and then click **OK**.

Creating and configuring an organizational group

Each organizational view contains one or more organizational groups, each of which may contain resources and child organizational groups. The hierarchical structure of organizational groups can have as many levels as you require to represent the way that resources are organized in your environment. The membership of an organizational group includes the resources that are contained in all of its child groups.

The Symantec Management Console has a predefined **Default** organizational view in which all resources are automatically placed. The default structure is a hierarchy of organizational groups that are based on resource type. You cannot add or remove organizational groups from the **Default** organizational view. All newly discovered resources are automatically placed into the appropriate group in the **Default** organizational view.

This task is a step in the process for configuring resource security.

See [“Configuring resource security”](#) on page 286.

To create and configure an organizational group

- 1 In the Symantec Management Console, on the **Manage** menu, click **Organizational Views and Groups**.
- 2 In the left pane, right-click the organizational view for which you want to add an organizational group and then click **New > Organizational Group**.
- 3 In the right pane, edit the name and the description of the organizational group.
Group names have no restrictions, so you may have multiple groups with the same name.
- 4 To add resources to the group, do the following:
 - In the right pane, click **Add**, and then click the item that you want to add to the group.

- In the **Edit Group** dialog box, select the appropriate resources, and then click **OK**.
- 5 To remove a resource from the group, right-click the resource and then click **Delete**.

Warning: When you delete a resource, it is removed from the CMDB. You should not delete any resources that are critical to the Symantec Management Platform activity and functionality. Critical resources include the Notification Server computer, sites, and subnets.

Viewing resources in an organizational group

The Resources panel displays all of the resources that are directly included in the organizational group, and all the resources that are included in any of its child groups. You can change the view to see only the computers that are in the group.

See [“Configuring resource security”](#) on page 286.

You can view the list of resources that are available for a particular security role. For example, you may want to verify that you have correctly set up the resource security for a particular role. The security roles that are assigned to an organizational group determine the access to all resources that are directly included in that group. Each security role has access to only the resources that are directly included in the groups to which the role is assigned.

When you view the resources for a particular security role, you see only the resources that are available for both the selected role and your role. If your role is the Administrator role (which has access to all resources), you always see all the resources that are available to the selected role. However, if you have another role (which may not have access to all resources), you may not see all of the resources that are available to the selected role.

Note: If you do not belong to a role (i.e. user-based security has been applied rather than role-based), choose **None** to have no security role selected. This ensures that all the resources to which you have access are shown. If you select a role that you do not belong to, all resources are filtered out and you will not see anything.

You can perform management actions on resources in an organizational group. The available actions include opening the Resource Manager, exporting the resource to an XML file, viewing the resource properties, adding the resource to a different group, and deleting the resource from the group.

To view resources in an organizational group

- 1 In the Symantec Management Console, on the **Manage** menu, click **Organizational Views and Groups**.
- 2 In the left pane, expand the **Organizational Views** folder and then select the appropriate organizational group.

- 3 (Optional) To view resources for a particular security role, in the right pane, under **Resources**, in the **Role** drop-down list, click the appropriate role.
- 4 (Optional) To export the list of resources into a spreadsheet or HTML file, do the following:
 - On the toolbar, click **Save As**, and then click the file format into which you want to export the data.
 - In the **Save As** dialog box, select if you want to export all resources, selected resources, or the resources that you filtered using the **Search** box, and then click **OK**.
 - In the **Save As** dialog box, select the folder in which to save the file, and then click **Save**.

Setting security on an organizational group

You set the security on an organizational group by assigning it the appropriate security roles. When a security role is assigned to a group, the members of that security role have access to the resources that are in the group. By default, all child groups inherit all security assignments on an organizational group. The inheritance gives the role the same access to all resources in those child groups. You can break the inheritance at any level, and can restore it when necessary.

To set security on organizational groups, you require the Change Permissions system permission.

When you install the Symantec Management Platform, the default configuration is that all roles have full permission on the **Default** organizational view. The default configuration gives all roles full access to all resources. If you want to configure resource security (which is optional), you can use the **Default** organizational view to set default permissions on all resources or particular types of resources. You need to break inheritance for the appropriate security roles and clear the permissions down the organizational group structure.

You can then assign a security role to an organizational group with the permissions that are appropriate for that role. For example, an administrator role would require full management rights to all resources in a group, but an end user role may require only read access to those resources. By default, assigning a security role some permissions on an organizational group gives that role the same permissions on all of its child groups.

This task is a step in the process for configuring resource security.

See [“Configuring resource security”](#) on page 286.

To set security on an organizational group

- 1 In the Symantec Management Console, on the **Manage** menu, click **Organizational Views and Groups**.
- 2 In the left pane, right-click the organizational group, click **Manage Security**, and then do one the following:

- | | |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To assign all available permissions | <ul style="list-style-type: none">■ Click Assign Management Rights.■ In the Assign Management Rights dialog box, select the appropriate security roles, and then click OK. |
| To assign the Symantec System "Read" permission | <ul style="list-style-type: none">■ Click Assign Read.■ In the Assign Read Rights dialog box, select the appropriate security roles, and then click OK. |
| To set custom security permissions | <ul style="list-style-type: none">■ Click Assign Custom.■ In the Security Role Manager, in the Role drop-down list, click the security role for which you want to set custom permissions.■ In the View drop-down list, click All Items.■ In the left pane, select the organizational view or group for which you want to set permissions.■ In the right pane, under Noninherited, make the appropriate changes to the permission settings.■ (Optional) If you want to configure permission inheritance, click Advanced.
See "Customizing permission inheritance" on page 79.■ Click Save changes. |

3 Click **Save changes**.

Considerations for resource scoping

Resource scoping provides a secure means of segregating resources into manageable, well structured units. These units are generic in nature so they can be arranged to suit a wide variety of organizational requirements.

In most cases assessing the resource scoping requirements within your design come down to the following questions:

- Who should have full access to the Symantec Management Platform infrastructure?
- What roles exist within the management functions of day to day operations?
- What areas of functionality require specific roles and rights?
- Does Active Directory accurately reflect our management and business model?
- Do Active Directory groups exist that reflect the roles within the Symantec Management Platform architecture?
- What are the types of resources that need to be managed?

When designing your resource framework, use the following implementation checklist to ensure that it is completed in the correct order:

- Identify users, security roles, and rights.
- Create security roles.
Assign rights, and assign user membership.
- Create organizational views and groups structure.
Follow AD Import best practices. Group by resource type (User, Computer).
- Assign roles and permissions to specific organizational views and groups.
- Generate reports for baseline system view of resources.
- Back up the organizational view and group structure using export XML.

Table 24-2 Design considerations for resource scoping

Item	Design considerations
Security	<ul style="list-style-type: none"> ■ You should set up security roles before performing any other console security tasks and before Notification Server is deployed to your production environment. ■ Resource security is the combination of Scope, Security Role, and Permissions. ■ Resources obtain all their permission grants from the scope collections that they are a member of. The grants are cumulative in nature. By having permission to perform an action on a resource in one scope collection, you ensure that the user/role can continue to perform this action regardless of whether the permission is applied to other scope collections containing the resource. ■ Security roles are the user groups that let you assign privileges for administrative and worker responsibilities and assign permissions for the folders or items that those administrators and workers can view in the Symantec Management Console. ■ Out-of-the-box roles are provided with a variety of privilege grants, and roles can be assigned anywhere within the organizational view or organizational group structure, depending on the administrative scope you choose to grant. ■ Security grants are assigned to organizational groups and are inherited from the organizational group above it.

Table 24-2 Design considerations for resource scoping (*continued*)

Item	Design considerations
Organizational views	<ul style="list-style-type: none"> ■ An organizational view is a self-contained secure hierarchy of organizational groups, which contain resources. ■ Organizational views provide a simplified and a secure means to group and manage resources. ■ Consider an organizational view to represent an administrative security structure or boundary which aligns with your IT environment. ■ Mirror your Active Directory organizational model by using Active Directory Import to avoid manual creation and population. ■ All resources in an organizational view (managed and unmanaged) are scoped by default. ■ Organizational views only contain resources through the organizational groups. An organizational view cannot contain any resources directly. All newly discovered resources are automatically imported into the default organizational view. ■ One resource item can belong to only one organizational group in each organizational view. When you add a resource to an organizational group, it is automatically removed from any other group to which it may be assigned. ■ Use organizational groups to apply a policy or task to selected computers, users, and resources. To do this, use an organizational group in a target. In this instance, an organizational group functions as a filter, but provides security to ensure that only the resource to which the target owner has permission is included. ■ Symantec Management Platform allows multiple organizational views because administrators may have multiple ways of organizing resources. Therefore, you can have both a view by function and by region. ■ With the default organizational view, all resources are scoped and secure in this view; resources (managed and unmanaged) are grouped by type, and the resource membership is dynamic. ■ Resource membership within the system default view is dynamically updated, and set at a 5-minute update interval. Depending on how you plan the creation and the resource membership of your organizational structure, keep this issue in mind when identifying the overall effect of resource membership updates.
Filters	<ul style="list-style-type: none"> ■ Filters are conceptually similar to Notification Server 6 collections. They are implemented differently as they are applied to targets, not policies. They are resources joined together by a defined set of criteria. ■ Filters should be created from a single attribute. Filters can be combined to create complex targets, and by using fewer criteria you get a higher chance of re-use and lower complexity, which results in a more efficient Notification Server.

Table 24-2 Design considerations for resource scoping (*continued*)

Item	Design considerations
Targets	<ul style="list-style-type: none"> ■ Targets are the intersection of organizational groups and filters. For example, all computers in the Finance (Group) that have less than 1GB RAM (Filter). ■ Targets are applied to policies and tasks and can be pre-created or created at the time of application. ■ Targets can only contain the resources that the target creator has access to. They are not visible as objects anywhere in the console, but are accessible using the Apply to option within a task or policy.

Configuring resource filters and targets

This chapter includes the following topics:

- [About resource filters](#)
- [Creating or modifying a filter](#)
- [Viewing filter dependencies](#)
- [About resource targets](#)
- [Creating a new target in ITMS Management Views](#)
- [Scheduling resource membership updates](#)

About resource filters

A filter, also known as a resource filter, is a dynamic definition of a set of resources. The resources may be grouped by some specified parameters, and they may also be explicitly included in a filter or excluded from a filter. A filter typically isolates only one aspect of a resource, such as its operating system, available disk space, or RAM. Filters are used with organizational groups to identify the resources (a resource target) that a task or policy applies to.

See [“About resource targets”](#) on page 312.

A filter does not contain any specific resources. All resources are contained in the organizational groups that are set up in organizational views. The organizational groups and organizational views are the same as are used for resource security. A filter operates on a specific organizational view or group to identify the appropriate resources. Consequently, filters are portable and can be applied to any organizational view or group, and they can be used with other filters. For example, you may want to apply a policy to all Windows XP computers in a

particular department of your organization. In this case, to select only the computers that run Windows XP, you can apply a filter to the organizational group that represents the appropriate department.

See [“Creating or modifying a filter”](#) on page 298.

Creating or modifying a filter

You can create a new filter from scratch, or clone an existing filter and modify it to suit your requirements. You can modify any filter that you have created or have write permission on. You cannot modify any of the default filters that are supplied with Notification Server. You cannot modify any of the filters that are added by hierarchy replication from a parent Notification Server. Only the filters that have been created on your Notification Server can be edited locally.

See [“About resource filters”](#) on page 297.

You can create the following types of filters:

- | | |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Query Builder filter | Filters the computers according to the criteria that you select. When you create a new filter, it is automatically created as a Query Builder filter. When you create a Query Builder filter, you can add the filter criteria from the default criteria list or create custom filter criteria. |
| SQL filter | Filters the computers according to the parameters that you define in the SQL editor. The SQL editor lets you modify the existing filters and create new ones.

See “Adding an SQL query to the filter in ITMS Management Views” on page 302.

Note: Filter evaluation may take a longer time depending on the complexity of SQL, specified criteria, and included filters. |
| Basic filter (Static filter) | Filters the computers according to the explicit criteria.

You can add the static lists of computers or filters. You can configure the filter details area to display only the explicit criteria.

You can include lists of computers or filters, or exclude them from the filter.

See “Adding explicit criteria to the filter in ITMS Management Views” on page 302.

Note: Symantec recommends that you do not use filters with the static lists that contain more than 1000 computers. When a filter contains a static list of 1000 computers or more, the evaluation of such a filter can take a long time. To include a static filter that contains 1000 or more computers, Symantec recommends that you use the SQL or the Query Builder filter. |

You can also create a filter by saving a report. A filter created this way is a static filter and has no query. The filter membership is a fixed list of inclusions that is determined when the filter

is created. You can modify a static filter by adding further inclusions or exclusions, which may be dynamic filters. However, you cannot add a query directly to a static filter.

See [“Creating a static filter from Notification Server report results”](#) on page 373.

Table 25-1 Process for creating or modifying a filter

Step	Action	Description
Step 1	Create a new filter or select an existing filter to modify.	<p>You can create a new filter from scratch, or modify an existing filter to suit your requirements.</p> <p>Note that you can quickly create a new filter in the ITMS Management Views or you can create a filter with more specific settings in the default filter tree.</p> <p>See “Creating a new filter in ITMS Management Views” on page 300.</p> <p>See “Creating a new filter in the default filter tree” on page 304.</p> <p>See “Modifying an existing filter in ITMS Management Views” on page 303.</p> <p>See “Modifying an existing filter” on page 309.</p>
Step 2	Select the query type.	<p>This step applies only to a new filter. You cannot change the query type when you modify an existing filter.</p> <p>If you want to create a dynamic filter, you need to select the appropriate query type. If you choose no query, the filter membership is the specified inclusions and exclusions.</p> <p>See “Selecting the filter query type” on page 305.</p>
Step 3	Specify the query to use.	<p>You can write the query SQL yourself or use the Query Builder to build the filter query. The Query Builder is a user-friendly tool that lets you select the tables and fields that you want to use. It helps you define the query to suit your requirements.</p> <p>See “Defining a resource query for a filter” on page 306.</p> <p>See “Defining an SQL query for a filter” on page 307.</p>
Step 4	Specify the inclusions and exclusions.	<p>You can specify particular resources or filters to include or exclude in the filter. The filters that you include or exclude may contain further filters. You can select from the resources and filters that are available in the CMDB, and you can import resources from a CSV file.</p> <p>See “Specifying filter inclusions and exclusions” on page 308.</p>

Table 25-1 Process for creating or modifying a filter (*continued*)

Step	Action	Description
Step 5	Verify the filter configuration by viewing the filter membership.	The membership of a filter is determined by running the filter query on the CMDB to extract the appropriate resources. You can update the membership to verify that the filter is correctly defined. See “Updating the membership of a filter” on page 310.
Step 6	Save the filter.	You can save the new filter definition or modified filter definition. Once a new filter is saved, you cannot change its query type. See “Creating a new filter in the default filter tree” on page 304. See “Modifying an existing filter” on page 309.
Step 7	(Optional) Save the filter data in a file.	You can save the filter data in a spreadsheet or HTML file. See “Saving the filter data in a file” on page 311.

Creating a new filter in ITMS Management Views

You can quickly create a new filter in ITMS Management Views.

See [“About resource filters”](#) on page 297.

See [“Creating or modifying a filter”](#) on page 298.

To create a new filter

- 1 In the Symantec Management Console, on the **Manage** menu, click **Computers**.
- 2 On the **Computers** view page, do one of the following:
 - In the content pane, under **Filters**, right-click, and then click **New > Filter**.
 - To create a new filter in a particular folder, right-click a folder, and then click **New > Filter**.
 - In the content pane, in the top left corner, click the **New Filter** symbol.
- 3 In the content pane, click **Add Filter Criteria**.
- 4 Depending on the type of filter that you want to create, do one of the following:
 - To edit a Query Builder filter, in the drop-down list, choose any criteria, and then, in the text box next to the criterion name, type the criterion value.
You can add as many criteria as necessary.
To add custom criteria to your filter, in the drop-down list, click **Edit Criteria List**. In the **Manage Filter Criteria** dialog box, you can choose data classes, associations and columns.

After you have chosen the custom criteria, in the content pane, in the **Add Filter Criteria** drop-down list, click the new query parameters that you have added, and then specify their value. If the parameter value is numerical, you can use comparison operators to combine these numbers.

After you configure the query and save it, it is automatically added to the filter, and the computer list in the content pane is automatically updated.

Note: The filter criteria are combined through the logical operator AND.

- To create a SQL filter, on the right from the **New Filter** symbol, click the **Edit SQL** symbol.
In the **Edit Raw SQL** dialog box, edit and test the query, and then click **OK** to save the newly created query.

Note: Filter evaluation may take a longer time depending on the complexity of SQL, specified criteria, and included filters.

- To add a static list of computers or filters, in the content pane, click the **Use only explicit criteria** symbol.
In the **Add Explicit Criteria** drop-down list, click one of the options to include or exclude a computer list or a filter. In the **Include/Exclude Computer List/Filter** dialog box, choose the items that you want to include or exclude, and then click **OK**.
If you want to see only the explicit criteria, in the content pane, next to the **Save Filter** symbol, click the **Use only explicit criteria** symbol.
- 5 After you have added the filter criteria, click the **Save Filter** or the **Save Filter As** symbol.
 - 6 (Optional) To compile a custom report, in the content pane, click the **View filter results report** symbol.
In the **Filter Results Report** dialog box, select the association, data classes and columns. To save the report configuration for the selected filter, at the bottom of the dialog box, check **Save the selected columns for filter**. The configuration is saved separately for each user and each filter. To export the report results as a CSV file, click **Export**.
 - 7 In the **Save Filter** or the **Save Filter As** dialog box, type the new name for the filter, choose if the filter should be displayed in the **Computers** view, and then click **OK**.

Note: If a filter with the same name already exists, you are prompted to overwrite the existing filter. If the filter that you have chosen to overwrite is a read-only filter, you need to either rename the filter or clone it. If you try to overwrite a filter that has dependencies, you are prompted to look at the list of dependencies first.

After you have created a filter, in the content pane, you see a dynamic list of computers based on the filter criteria that you have added.

Adding an SQL query to the filter in ITMS Management Views

You can create the queries and run them directly on the SQL server. You can also create filters based on these queries.

See [“About resource filters”](#) on page 297.

See [“Creating a new filter in ITMS Management Views”](#) on page 300.

Warning: To create or edit an SQL query, you need to have the **Edit SQL Directly** system privilege.

To add an SQL query to the filter in ITMS Management Views

- 1 In the Symantec Management Platform, on the **Manage** menu, click **Computers**.
- 2 In the navigation pane, under **Filters**, click the filter that you want to configure.
- 3 In the content pane, in the upper right corner, click the double arrows to expand the filter details, and then click the **Edit SQL** symbol.
- 4 In the **Edit Raw SQL** dialog box, write an SQL query, or paste an existing query, and then click **Test query**.

If the query that you have configured is incorrect, the **Results** box displays an error message. You cannot save an incorrect query.

If the query is correct, the **Results** box displays a list of computers.

Note: Filter evaluation may take a longer time depending on the complexity of SQL, specified criteria, and included filters.

- 5 Click **Close**.
- 6 Click the **Save Filter** symbol.
- 7 In the **Save Filter** dialog box, specify the name and the location of the filter, and then click **OK**.

Adding explicit criteria to the filter in ITMS Management Views

You can include filters or lists of resources to the filter, or exclude them.

See [“About resource filters”](#) on page 297.

See [“Creating a new filter in ITMS Management Views”](#) on page 300.

Warning: Symantec recommends that you do not use filters with the static lists that contain more than 1000 computers. When a filter contains a static list of 1000 computers or more, the evaluation of such a filter can take a longer time than usual. To include a static filter that contains 1000 or more computers, Symantec recommends that you use the SQL or the Query Builder filter.

To add explicit criteria to the filter in ITMS Management Views

- 1 In the Symantec Management Platform, on the **Manage** menu, click **Computers**.
- 2 In the navigation pane, under **Filters**, click the filter that you want to configure.
- 3 In the content pane, in the upper right corner, click the double arrows to expand the filter details.
- 4 Click **Add Explicit Criteria** list, and then click **Include Filter** or **Include List**.
In the **Include Filter** or **Include Computer List** dialog box, use the arrows to move the resources between the columns.
Click **OK**.
- 5 (Optional) Click **Exclude Filter** or **Exclude List**.
In the dialog box that opens, choose the filter or computers that you want to exclude, and then click **OK**.
- 6 (Optional) To view only the explicit criteria, in the content pane, click the **Use only explicit criteria** symbol.
- 7 Click the **Save Filter** symbol.
- 8 In the **Save Filter** dialog box, specify the name and the location of the filter, and then click **OK**.

Modifying an existing filter in ITMS Management Views

You can modify any filter that you have created.

See [“Creating or modifying a filter”](#) on page 298.

To modify an existing filter in ITMS Management Views

- 1 In the Symantec Management Console, on the **Manage** menu, click **Computers**.
- 2 In the content pane, in the **Filters** tree, click the filter that you want to modify.
- 3 In the content pane, click the double arrows to view the filter details, and then do one of the following:

- To add filter criteria, expand the **Add Filter Criteria** list, click a criterion then you want to add, and then specify the criterion value.
You can add as many criteria as you need.
 - To add custom filter criteria, expand the **Add Filter Criteria** list, and then click **Edit Criteria List**.
In the **Add Filter Criteria** dialog box, choose the associations, data classes, and columns, and then click **OK**.
In the **Add Filter Criteria** list, click the newly added custom criteria, and then specify the criteria value.
 - To edit the SQL query, in the upper left corner, click the **Edit SQL** symbol.
In the **Edit Raw SQL** dialog box, edit the SQL query, and then click **Test query**. If the test is successful, click **Close**.
 - To specify the filter inclusions and exclusions, expand the **Add Explicit Criteria** list, and then configure the inclusions and exclusions according to your need.
To view only the filter inclusions and exclusions, in the upper left corner of the pane, click the **Use only explicit criteria** symbol.
- 4 (Optional) To compile a custom report, in the content pane, click the **View filter results report** symbol.
- In the **Filter Results Report** dialog box, select the association, data classes and columns. To save the report configuration for the selected filter, at the bottom of the dialog box, check **Save the selected columns for filter**. The configuration is saved separately for each user and each filter. To export the report results as a CSV file, click **Export**.
- 5 Click the **Save Filter** or **Save Filter As** symbol.
- In the **Save Filter As** dialog box, specify the name and the location for the filter, and then click **OK**.

Creating a new filter in the default filter tree

You can create any new filters that you need, and you can specify the query, inclusions, and exclusions to define the membership that you want.

See [“About resource filters”](#) on page 297.

This task is a step in the process for creating or modifying a filter.

See [“Creating or modifying a filter”](#) on page 298.

To create a new filter in the default filter tree

- 1 In the Symantec Management Console, on the **Manage** menu, click **Filters**.
- 2 In the left pane, right-click the folder to which you want to add the new filter, and then click **New > Filter**.

- 3 In the right pane, specify the filter name and description.
- 4 Select the query type.
See [“Selecting the filter query type”](#) on page 305.
- 5 Do any of the following actions:

Define the query	See “Defining a resource query for a filter” on page 306.
	See “Defining an SQL query for a filter” on page 307.
Specify any necessary inclusions and exclusions	See “Specifying filter inclusions and exclusions” on page 308.
Update the filter membership	See “Updating the membership of a filter” on page 310.
- 6 Click **Save Changes**.

Selecting the filter query type

When you create a new filter, you need to specify the type of query to use. You can use the Query Builder to define the filter query, or you can write the query SQL yourself. You can also choose to have no query in the filter. You cannot change the query type after the filter has been saved.

See [“About resource filters”](#) on page 297.

This task is a step in the process for creating or modifying a filter.

See [“Creating or modifying a filter”](#) on page 298.

To select the filter query type

- 1 In the Symantec Management Console, on the **Manage** menu, click **Filters**.
- 2 In the left pane, right-click the folder to which you want to add the new filter, and then click **New > Filter**.
- 3 On the **New Filter** page, in the **Filter Definition** drop-down list, select the query type that you want to use:

None	The filter does not use a query. The inclusions and exclusions of specific resources and filters defines the filter membership.
Query Builder	Use the Query Builder to build the filter query. The Query Builder is a user-friendly tool that lets you select the tables and fields that you want to use. It helps you define the query to suit your requirements. See “Defining a resource query for a filter” on page 306.
Raw SQL	Write your own SQL query. For example, you may want to copy a query from another filter or report and modify it to suit your requirements. See “Defining an SQL query for a filter” on page 307.

Defining a resource query for a filter

A resource query is based on the tables that are available in the CMDB. The Query Builder is a user-friendly tool that provides a standard template and lets you select the tables and fields that you want to use. It helps you to define the query to suit your requirements. You do not need any SQL knowledge to define a resource query. The resource query is converted to SQL automatically, and the SQL is run on the CMDB to extract the appropriate resources.

See [“Selecting the filter query type”](#) on page 305.

This task is a step in the process for creating or modifying a filter.

See [“Creating or modifying a filter”](#) on page 298.

To define a resource query for a filter

- 1 In the Symantec Management Console, on the **Manage** menu, click **Filters**.
- 2 In the left pane, click the filter that you want to modify.
- 3 In the right pane, in the **Filter Definition** panel, specify the resource query details on the appropriate tabs.

Query	The resource query syntax.
Fields	The fields and the data class attributes to use in the query.
Query Parameters	<p>The parameters that are used in the query. These are internal parameters for SQL use, not user parameters.</p> <p>Parameters are not commonly used in filter queries, but may be useful for getting registry information. For example, an agent version number for an upgrade.</p>
Filter Expressions	<p>The conditional statements that are used to further refine the results of the query. Each statement or grouped statement can be considered a filter. You need to create the statements that you want to use and group them accordingly.</p>
Resolved Query	The SQL code that is run on the CMDB to extract the filter results.

Defining an SQL query for a filter

You can write an SQL query to define the resources that you want to include in the filter. You can write the SQL code from scratch. Alternatively, you can copy the SQL from another filter or report and modify it to suit your requirements. For example, you can create a resource query using the Query Builder, and then copy the generated SQL from the Resolved Query tab. You can also use the Query Builder to define the basic structure of your query, convert it to SQL, and then modify the SQL directly to create the query that you want.

You need the Edit SQL privilege to create or modify SQL queries, and you should have a good understanding of the CMDB table structure.

See [“Selecting the filter query type”](#) on page 305.

This task is a step in the process for creating or modifying a filter.

See [“Creating or modifying a filter”](#) on page 298.

To define an SQL query for a filter

- 1 In the Symantec Management Console, on the **Manage** menu, click **Filters**.
- 2 In the left pane, click the filter that you want to modify.
- 3 In the right pane, in the **Filter Definition** panel, specify the SQL query details on the appropriate tabs.

Parameterized Query The SQL code for the query.

Query Parameters The parameters that are used in the query. These are internal parameters for SQL use, not user parameters.

Parameters are not commonly used in filter queries, but may be useful for getting registry information. For example, an agent version number for an upgrade.

Resolved Query The SQL code that is run on the CMDB to extract the filter results.

- 4 Click **Save Changes**.

Specifying filter inclusions and exclusions

You can specify particular resources or filters to include or exclude in your filter. The filters that you include or exclude may contain further filters. You can select resources and filters from the list of those available in the CMDB, and you can also import resources from a .csv file.

If you import resources from a .csv file, the file may identify a computer by name, fully qualified domain name, or IP address. Any item that is not found in the CMDB is ignored.

The filter membership is determined by adding the inclusions to the query results, and then removing the exclusions. Filters and resources have no difference in priority.

This task is a step in the process for creating or modifying a filter.

See [“Creating or modifying a filter”](#) on page 298.

To specify resources to include or exclude

- 1 In the Symantec Management Console, on the **Manage** menu, click **Filters**.
- 2 In the left pane, click the filter that you want to modify.
- 3 In the right pane, in the **Filter Definition** panel, under **Explicit Inclusions and Exclusions**, do any of the following:

- | | | |
|----------------------------------------------------|---|------------------------------------------------------------------------------------------------------------------|
| To include selected resources | 1 | Under Inclusions , click Select a resource . |
| | 2 | In the Select Resources window, select the resources that you want to include, and then click OK . |
| To include the resources that are listed in a file | 1 | Under Inclusions , click Import from a file . |
| | 2 | In the Select File to Import window, select the appropriate CSV file, and then click Open . |
| To exclude selected resources | 1 | Under Exclusions , click Select a resource . |
| | 2 | In the Select Resources window, select the resources that you want to exclude, and then click OK . |
| To exclude the resources that are listed in a file | 1 | Under Exclusions , click Import from a file . |
| | 2 | In the Select File to Import window, select the appropriate CSV file, and then click Open . |

The selected resources are listed beside the appropriate fields.

To specify filters to include or exclude

- 1 In the Symantec Management Console, on the **Manage** menu, click **Filters**.
- 2 In the left pane, click the filter that you want to modify.
- 3 In the right pane, in the **Filter Definition** panel, under **Explicit Inclusions and Exclusions**, do any of the following:

- | | | |
|-----------------------------|---|--------------------------------------------------------------------------------------------------------------|
| To include selected filters | 1 | Under Inclusions , click Select a filter . |
| | 2 | In the Select Filters window, select the filters that you want to include, and then click OK . |
| To exclude selected filters | 1 | Under Exclusions , click Select a filter . |
| | 2 | In the Select Filters window, select the filters that you want to exclude, and then click OK . |

The selected filters are listed beside the appropriate fields.

Modifying an existing filter

You can modify any filter that you have created or that you have write permission on. You cannot modify any of the default filters that are supplied with Notification Server. You cannot modify any filters that are added by hierarchy replication from a parent Notification Server. Only the filters that were created on your Notification Server can be edited locally. The only action that you can perform on a read-only filter is to update the filter membership.

See [“About resource filters”](#) on page 297.

If you want to modify a read-only filter, clone it to create a new filter, and then modify the new filter to suit your requirements. When you modify a filter, you can modify the filter query and the specific inclusions or exclusions, but you cannot change the query type.

This task is a step in the process for creating or modifying a filter.

See [“Creating or modifying a filter”](#) on page 298.

To modify an existing filter

- 1 In the Symantec Management Console, on the **Manage** menu, click **Filters**.
- 2 In the left pane, click the filter that you want to modify.
- 3 (Optional) In the right pane, change the filter name and description.
- 4 In the upper-right corner, click **Edit**.

If the Edit option is unavailable, the filter is read-only and you cannot modify it.

- 5 Do any of the following actions:

Modify the query See [“Defining a resource query for a filter”](#) on page 306.

 See [“Defining an SQL query for a filter”](#) on page 307.

Modify the inclusions and See [“Specifying filter inclusions and exclusions”](#) on page 308.
exclusions

Update the filter membership See [“Updating the membership of a filter”](#) on page 310.

- 6 Click **Save Changes**.

Updating the membership of a filter

The membership of a filter is determined by running the filter query on the CMDB to extract the appropriate resources. To keep the filter membership up-to-date as the resource information in the CMDB changes, you should update the membership at suitable intervals. You can use the scheduled filter updates to update the filter membership, or you can run the update manually at appropriate times. For example, when you create or modify a filter, you can update the membership to verify that the filter is correctly defined.

See [“About resource filters”](#) on page 297.

See [“Scheduling resource membership updates”](#) on page 315.

The Filter Membership panel on the *Filter Name* page shows details of the resources in your scope that are currently identified as members of the filter. The filter membership may be different for different user roles. Only the resources that a user has Read permission on are visible to that user. However, when a user manually updates the membership of a filter, the

filter query is run on all resources in the CMDB. The console restricts the results to show only the resources that are within the viewing user's scope.

This task is a step in the process for creating or modifying a filter.

See [“Creating or modifying a filter”](#) on page 298.

To update the membership of a filter

- 1 In the Symantec Management Console, on the **Manage** menu, click **Filters**.
- 2 In the left pane, click the filter for which you want to update the membership.
- 3 In the right pane, in the **Filter Membership** panel, do any of the following:

To update the filter membership immediately

Click **Update Membership**.

To update the filter membership using the filter update schedules

Click **Update Membership > Auto**.

To allow manual filter membership updates only

Click **Update Membership > Manual**.

This option turns off the scheduled updates for the filter membership. For example, the filter contains a complex query that you want to run only when necessary.

Saving the filter data in a file

You can export the data of the default or custom filters into a spreadsheet or HTML file. Depending on your needs, you can export all data, or only selected or filtered items.

This task is an optional step in the process for creating or modifying a filter.

See [“Creating or modifying a filter”](#) on page 298.

To save the filter data in a file

- 1 In the Symantec Management Console, on the **Manage** menu, click **Filters**.
- 2 In the left pane, click the filter for which you want to save the data.
- 3 In the right pane, in the **Filter Membership** panel, click **Save As**, and then click the file type that you want.
- 4 In the **Save As** dialog box, select the data range, and then click **OK**.

Viewing filter dependencies

Before you modify a filter, you may want to find out what other items depend on it. You can view a list of all the filters, targets, tasks, and policies that use a particular filter.

See [“About resource filters”](#) on page 297.

The list of dependencies contains all of the targets that include the specified filter directly or within an included filter. The list also contains all policies and tasks that are applied to those targets. The inclusion of the filter in the target defines the dependency. The dependency does not necessarily mean that the policy or task is currently applied to a resource in the filter.

To view the dependencies of a filter

- 1 In the Symantec Management Console, on the **Manage** menu, click **Filters**.
- 2 In the left pane, click the filter for which you want to view dependencies.
- 3 In the right pane, in the **Filter Membership** panel, click **Referenced By**.
- 4 In the **Items applied to this filter** dialog box, view the list of filters, targets, tasks, and policies that use the filter.
- 5 Click **Close**.

About resource targets

A resource target, usually known as a target, is a framework that lets you apply tasks and policies to a dynamic collection of resources. A target consists of at least one organizational view or group, and a number of filters. The filters refine the available resources to identify those that you want. The organizational view or group acts as a security filter. It ensures that the policy or task is applied only to resources that the user's security role has permission to work with.

See [“Creating a new target in ITMS Management Views”](#) on page 314.

Targets are cached in the CMDB and dynamically evaluated when the task or policy is run. The target is evaluated against the scope of the current user. Only the resources that appear in the organizational view or group and in the filters are returned. The target includes only the resources to which the user has Read access. Resources outside the current user's scope are never visible.

The system filters that are supplied with Notification Server contain only managed resources, but targets and organizational views and groups may contain unmanaged resources. You can also create your own custom filters that include unmanaged resources. However, when you apply a target to a policy or task, only the managed computers in the target can request the policy or run the task.

There are two types of targets that you can apply to a policy or task:

- Autogenerated resource targets

These are targets that have not been explicitly named and saved. Autogenerated targets are used only by the policy or task in which you create them. For example, if you use the **Apply to** option to select a filter, or the Select Resources dialog box to select a set of resources, the corresponding target is created and added to the policy or task. The autogenerated target is given a default name that is based on the organizational group, filter, or set of resources that it contains.

You can edit these targets when you modify the policy or task, but you cannot apply them to any other policies or tasks.
- Named resource targets

These are targets that have been explicitly saved as named resource targets. Named targets can be applied to any number of tasks and policies, and can be modified by any user that has the appropriate permissions.

In the ITMS Management Views, you can see the **Targets** list. The following folders are displayed by default:

Table 25-2 Folders in the Targets list

Folder	Description
Favorites	A folder where you can store the most commonly used targets. Each user can create their own list of commonly used filters and arrange them in the Favorites folder.
System	A folder that contains all the system targets grouped according to the solutions that they belong to.

The color code that is used to mark different types of targets is as follows:

Table 25-3 Color codes

Color	Target type
Gray	A saved target that is not assigned to a task or policy.
Red	A saved target that is assigned to an inactive task or a policy that is turned off.
Green	A saved target that is assigned to an active task or a turned on policy.

Note: The targets that you create on demand from policies and tasks and do not save specifically, are not displayed in the **Targets** list.

See [“About resource filters”](#) on page 297.

See [“Creating or modifying a filter”](#) on page 298.

Creating a new target in ITMS Management Views

When you create a new target, it is always empty and it is always created in the parent folder by default.

If you want to modify a target in the **System** folder, you need to clone the target first.

You can create target from any filter using the right-click menu.

The targets that were created in the older version of the Console views can be shown as incompatible targets, so that you cannot modify them in the new interface. To edit such a target, in the content pane, click the **Incompatible Target** link. A legacy user interface opens, and you can edit the target there.

See [“About resource targets”](#) on page 312.

To create a new target in ITMS Management Views

- 1 In the Symantec Management Console, on the **Manage** menu, click **Computers**.
- 2 In the navigation pane, expand the **Targets** section, and then do one of the following:
 - In the **Targets** tree, right-click, and then click **New > Target**.
In the **Target** dialog box, type a name for the new target, and then click **OK**.
 - In the **Filters** tree, right-click a filter, and then click **Create Target from Filter**.
In the **Create Target from Filter** dialog box, type a name for the new target, and then click **OK**.
- 3 In the content pane, on the right form the **Search** box, click the double arrows to expand the target details, and then click **Add Include/Exclude**.
- 4 In the **Add Include/Exclude** drop-down list, click **Include** to add a parameter, and then, in the drop-down list that appears on the right, click one of the following:
 - **Filter**
 - **Group**
 - **List**

The criteria are evaluated in the same order as they appear on the page.

The first criterion must always be **Include**.

- 5 (Optional) You can include as many additional parameters as necessary. You can include the following additional parameters:
 - **Include Only**
Lets you view intersecting values of several filters.
 - **Exclude**

Lets you exclude a computer from the target.

6 Click the **Save Target** symbol, and then, in the **Save Target** dialog box, click **OK**.

After you have created a target, in the content pane, you see a dynamic list of computers based on the target criteria that you have added.

Scheduling resource membership updates

You can keep all of your resource filters, organizational groups, and resource targets up to date by configuring the appropriate filter update schedules. These schedules let you update the filters, organizational groups, and targets that you need at suitable intervals. These schedules help you manage the processing load that is imposed on Notification Server.

See “[About resource filters](#)” on page 297.

Predefined resource membership update schedules are supplied with the Symantec Management Platform. These schedules are suitable for most purposes and you should not need to change them. However, as the requirements of your organization change, you can make the necessary changes.

Table 25-4 Resource membership update schedules

Schedule	Description
Delta Update schedule	<p>Updates the membership of the following:</p> <ul style="list-style-type: none"> ■ Filters that have had membership changes since the last update. ■ All dynamic organizational groups. ■ All invalid targets. <p>A target may be invalidated by the following events:</p> <ul style="list-style-type: none"> ■ Its definition is saved. ■ A filter that it uses has membership changes. ■ An organizational group that it uses has membership changes. ■ The security that is applied to an organizational group that it uses changes. <p>By default, this schedule runs every five minutes.</p>
Complete Update schedule	<p>Completely re-creates the membership of all filters, organizational groups, and targets, regardless of inventory status or any changes to policies. The complete update may impose a significant load on Notification Server and should be scheduled accordingly.</p> <p>By default, this schedule once a day.</p>

Table 25-4 Resource membership update schedules (*continued*)

Schedule	Description
Policy Update schedule	<p>Updates the membership of filters that a policy uses, if the policy has changed since the last update.</p> <p>This schedule ensures that when you update or create a policy, all the filters that are included in the new policy targets or modified policy targets are updated automatically.</p> <p>By default, this schedule runs every five minutes.</p>

See [“Components of a Symantec Management Platform schedule”](#) on page 91.

See [“Viewing the Notification Server internal schedule calendar”](#) on page 95.

To configure the resource membership update schedules

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Resource Membership Update**.
- 2 On the Resource Membership Update page, configure the update schedules that you want to use.
 See [“Specifying a policy schedule”](#) on page 326.
- 3 If you want to run an update schedule immediately, in the appropriate panel, click **Run**.
 For example, you can ensure that all the changes to your filters take effect immediately, rather than waiting until the scheduled update.
- 4 Click **OK**.

Configuring packages

This chapter includes the following topics:

- [Editing the configuration settings for a package](#)
- [Updating the distribution points for a package](#)
- [Enabling access to a package at a UNC source location](#)

Editing the configuration settings for a package

A package includes a set of files that can be delivered to a managed resource. For example, the Symantec Management Agent Package includes the AeXClientUpgrade.exe file. The AeXClientUpgrade.exe file installs the agent to managed resources.

The **Package** page lets you configure the package settings, such as package source, package location, and how the package runs.

To edit the configuration settings for a package

- 1 In the Symantec Management Console, on the **Manage** menu, click **Organizational Views and Groups**.
- 2 In the left pane, expand **Default**, and then click **Package**.
- 3 On the **Package** page, right-click the package that you want to edit, and then click **Actions > Edit Package**.
- 4 In the **Add or Edit Package** dialog box, make the necessary configuration changes on the appropriate tabs, and then click **OK**.

For more information, click the page and then press **F1**.

You need to update the package distribution points to update the package information on each package server.

See [“Updating the distribution points for a package”](#) on page 318.

Updating the distribution points for a package

Package distribution points are the locations where the package is stored, such as package servers or UNC source locations. Information on each package is contained in an XML file that is stored with the package. This information must be updated each time the package is modified. Notification Server and package servers use this information to provide the appropriate files when a managed computer requests the package. The package information is updated on a schedule, but you can perform a manual update when needed. For example, you can manually update the distribution points for a modified package to immediately update the package information on all of its distribution points.

See [“Editing the configuration settings for a package”](#) on page 317.

To update the package distribution points for a package accessed from the Settings menu

- 1 In the Symantec Management Console, on the **Manage** menu, click **Organizational Views and Groups**.
- 2 In the left pane, expand **Default**, and then click **Package**.
- 3 On the **Package** page, right-click the package for which you want to update the distribution points, and then click **Update Distribution Points**

Enabling access to a package at a UNC source location

The Symantec Management Agent uses the agent connectivity credential (ACC) to connect to IIS on Notification Server to download UNC packages through HTTP. IIS then authenticates to the UNC source using the distribution point credential (DPC). The Symantec Management Agent uses the ACC to connect to download sources. Ensure that ACC has read access when the Symantec Management Agent downloads directly from the UNC package source.

The DPC is not used if the Symantec Management Agent downloads a package from a package server. The package server applies either anonymous access or the ACC to the downloaded package files.

To enable access to a package at a UNC source location

- 1 Specify the package distribution point credentials that you want to use.

You specify these credentials on the **Distribution Point Credentials** tab of the **Notification Server Settings** page. Symantec recommends that you select **Use Agent Connectivity Credential** when you specify the package distribution point credentials. This option ensures that only one credential, the ACC, needs to exist on UNC package source locations.

See [“Distribution point credential settings”](#) on page 53.

- 2 Give these credentials Read access on the UNC source folder.

Using policies

This chapter includes the following topics:

- [About Symantec Management Platform policies](#)
- [About user-based policies](#)
- [Managing Symantec Management Platform policies](#)
- [Pushing a policy in real time](#)
- [Specifying the targets of a policy or task](#)
- [Creating or modifying a resource target](#)
- [Specifying filtering rules for resource target](#)
- [Specifying a policy schedule](#)
- [About automation policies](#)
- [Key components of automation policies](#)
- [Managing automation policies](#)
- [Creating or modifying scheduled automation policies](#)
- [Creating or modifying message-based automation policies](#)
- [Creating and modifying automation policy tasks](#)
- [Disabling or limiting Notification Server Event processing for a client computer](#)

About Symantec Management Platform policies

A Symantec Management Platform policy is a set of rules that apply to a resource or a set of resources (known as the policy target). A policy may be evaluated on the basis of a schedule

or on the basis of the incoming data. When a policy is evaluated, the appropriate action is taken. This action typically includes running tasks on the target resources to ensure that they all comply with the policy.

Table 27-1 Common Symantec Management Platform policy types

Policy type	Description
Agent policies	Specifies the Symantec Management Agent configuration settings on client computers. See “Configuring the Symantec Management Agent using the configuration policies” on page 235.
Automation policies	Specifies automated actions to perform on client computers or on the Notification Server computer. Automation policies are dynamic. When a policy is activated, it targets the client computers, and performs the required actions according to the current state of each target computer. Automation policy targets may be specified according to the results of a report or a query, rather than according to filters and resource targets, as it happens with other policy types. See “About automation policies” on page 327.
Solution policies	Solutions have their own policies that target the client computers or the users of those solutions.
User -based policies	Specifies the settings that apply to particular users. These settings are applied to the computers that the users are logged into. See “About user-based policies” on page 320.

About user-based policies

User-based policies can be applied to specific users or groups of users. They may (but not necessarily) also be applied to specific computers.

See [“About Symantec Management Platform policies”](#) on page 319.

For example, some organizations have a large number of Active Directory security groups and want to assign their policies using these security groups. The security groups that contain managed computers or users are imported into the CMDB. Using user-based policies enables the administrator to manage computers using the existing Active Directory infrastructure. Workgroups and local users are supported.

User-based policies apply only when the user is logged on to a managed computer. These policies apply only to the user who is logged on to the console session. Each time a user logs on to a managed computer, the Symantec Management Agent searches for the user-based policies that apply to that user. Policies are cached on the computer for a week. The Symantec Management Agent also performs regular configuration requests for any active policies that

use the current logged on user's SID, in addition to the managed computer GUID, to receive both user-based and computer-based policies. The agent makes this request the first time that a user logs onto a managed computer. The agent repeats the request every time that it performs its normal configuration request.

Note: Users who are logged on to managed computers through terminal services do not receive the policies that target them. All the users see the policies that apply to the user who is logged on to the console session.

You may want to exclude some computers or users from user-based policies. For example, a managed computer that many users share, or an administrator who may log on to many different computers every day. If such a computer or user was a target for a user-based policy, the frequent policy-driven changes could impose significant overhead on the affected computers.

You can create a list of computers to which user-based policies do not apply. You can create a list of users to whom user-based policies should not be targeted. You can use these lists as exclusions in the appropriate filters.

See [“About resource filters”](#) on page 297.

See [“Creating or modifying a filter”](#) on page 298.

Managing Symantec Management Platform policies

The Policies view gathers all of the available policies in a single folder structure. This standard structure lets you easily access the policies that you want to view or modify.

See [“About Symantec Management Platform policies”](#) on page 319.

See [“About automation policies”](#) on page 327.

To manage policies

- 1 In the Symantec Management Console, in the **Manage** menu, click **Policies**.
- 2 In the left pane, under the Policies folder, select the policy or group of policies that you want to manage.

Pushing a policy in real time

You can select any policy and push it immediately to the client computers that belong to the target of this policy. The policy is then immediately delivered to the client computers, but it runs according to the schedule that is specified in the policy.

See [“About Time Critical Management”](#) on page 41.

Note: You can only push the policies that are enabled and that have a target configured.

The policy is pushed only to the client computers that are connected to Notification Server using the persistent connection.

See [“About the Symantec Management Agent communication using persistent connection”](#) on page 147.

If on the next get client policy request, the policy is disabled or the computer falls out of the target, the policy is deleted as regular policy.

To push a policy in real time

- 1 In the Symantec Management Console, on the **Manage** menu, click **Policies**.
- 2 In the navigation pane, right-click the policy that you want to push to the client computer, and then click **Push Policy**.

Note that by default, only **Symantec Administrators** role has the privilege for the push policy action.

Specifying the targets of a policy or task

You need to specify one or more targets for a policy or task. A target defines the computers, users, and resources to which the policy or task applies. A policy or task may have multiple targets.

See [“About resource targets”](#) on page 312.

To specify the targets of a policy or task

- 1 In the Symantec Management Console, navigate to the required policy or task.
- 2 On the policy or task page, under **Applied to**, click **Apply to**, and then click one of the following options:

Targets

- 1 In the **Select a resource target** dialog box, under **Available targets**, select a target or targets that you want to assign to the policy.
- 2 Click the arrow to move the targets to the **Selected targets** section, and then click **OK**.

See [“Creating or modifying a resource target”](#) on page 323.

Recently used targets

Lets you select recently used targets. This option immediately adds the target to the policy or task.

You can add as many targets as you want.

- 3 If you want to modify or delete a target from the list, select it in the **Applied to** grid, and then click **Edit** or **Delete**, whichever is appropriate.
- 4 Click **Save changes**.

Creating or modifying a resource target

The **Select computers** and **Edit selected group** windows let you select the items that you want to include in a new resource target.

See [“Specifying the targets of a policy or task”](#) on page 322.

To create or modify a resource target

- 1 In the Symantec Management Console, navigate to the required policy or task.
- 2 On the policy page or task page, under **Applied to**, click **Apply to > Targets**.
- 3 In the **Select a resource target** dialog box, do one of the following:

Create a new target.

- 1 Under **Available targets**, click **New > Target**.
- 2 In the **Select computers** dialog box, type the name of the target and configure the scoping of the target.
- 3 Under **Filtering Rules**, specify the rules to filter the available computers.

To include in the target only the computers that have Symantec Management Agent installed, check the **Include only managed computers** box.

See [“Specifying filtering rules for resource target”](#) on page 324.
- 4 When the **Computers currently matching rules** list shows the items that you want to include in the target, click **OK**.

Edit an existing target.

- 1 Under **Available targets**, select a target, and then click **Edit**.
- 2 In the **Edit selected target** dialog box, type the name of the target and configure the scoping of the target.
- 3 Under **Filtering Rules**, specify the rules to filter the available computers.

See [“Specifying filtering rules for resource target”](#) on page 324.
- 4 Click **OK**.

- Clone an existing target.
- 1 Under **Available targets**, select a target, and then click **Edit**.
 - 2 In the **Edit selected target** dialog box, check the **Clone** box, and then type the new name of the target.
 - 3 (Optional) Configure the scoping and filtering rules of the target.
 - 4 Click **OK**.

Configure the scoping of the target.

The scoping feature lets the administrator prepare the targets and share them with the users with low-privileged roles. The targets only contain the resources that are accessible to the members of the selected roles.

- 1 Under **Available targets**, create a new target or open an existing target for editing.
- 2 In the target builder dialog box, click the link that lists current scoping.

When you create a new target, the scoping contains all roles to which current user account belongs.

When you edit an existing target, the scoping contains the roles that are saved for this target previously.

- 3 In the **Select scoping roles** dialog box, under **Available resources**, select the security role(s) that you want to add to the scoping of this target.
- 4 Click the arrow to move the roles to the **Selected resources** section, and then click **OK**.
- 5 In the target builder dialog box, click **OK**.

Note: Note that full access to the target is only available to the account that is member of all selected security roles. For example, if **Level 1 Workers** and **Level 2 Workers** roles are selected for scoping, the account must be member of both roles to fully manage the target.

The specified resource target is added to the policy or task. If the target is autogenerated, it is given a default name that is based on the names of the organizational groups and filters that it uses.

Specifying filtering rules for resource target

The filtering rules let you filter computers, users, and resources to identify the items that you want to select. The rules are applied in the order in which they are listed, so any excluded items may be included again by a later rule. The **Items currently matching rules** list shows the items that the specified rules have selected.

Note that the list contains only the resources that are accessible to the members of the roles that are displayed under **Scoping**.

The list is updated automatically as you add and modify the filtering rules.

See “[Specifying the targets of a policy or task](#)” on page 322.

See “[Creating or modifying a resource target](#)” on page 323.

To specify a filtering rule for resource target

- 1 In the **Select Items** window, under **Filtering Rules**, click **Add rule**.
- 2 In the first drop-down list, click the appropriate operation:

Exclude items in	Excludes the items that are in the specified filter or organizational group, or selected resources from the item list.
-------------------------	------------------------------------------------------------------------------------------------------------------------

Exclude items not in	Excludes the items that are not in the specified filter or organizational group, or selected resources from the item list.
-----------------------------	----------------------------------------------------------------------------------------------------------------------------

- 3 In the second drop-down list, click the appropriate option:

Filter	Apply the operation to a specific filter.
---------------	-------------------------------------------

Group	Apply the operation to a specific organizational group.
--------------	---------------------------------------------------------

Item List	Apply the operation to specified computers, users, or resources.
------------------	------------------------------------------------------------------

- 4 In the third drop-down list, select the appropriate item:

To select a filter or group.	Type the first few letters of the filter or organizational group that you want. The options on the list are reduced to those that match.
------------------------------	------------------------------------------------------------------------------------------------------------------------------------------

To select specific items.	Click the ellipses (...) and then, in the Select Item window, select the appropriate items.
---------------------------	----------------------------------------------------------------------------------------------------

- 5 (Optional) To move a rule up or down the list of filtering rules, click the up arrow or down arrow.
- 6 (Optional) To remove a filtering rule from the list, click **Delete**.

- 7 (Optional) To only include in the target the computers that have Symantec Management Agent installed (managed computers), check the **Include only managed computers** box.

Note that this check box is only displayed when the target filtering rules start with **Computer** scope collection.

- 8 Click **OK**.

Specifying a policy schedule

You need to specify the times that a policy is triggered by configuring the appropriate schedules. You can specify as many schedules as you need, and can have any number active at once.

See [“About Symantec Management Platform policies”](#) on page 319.

To specify a policy schedule

- 1 On the policy page, under **Schedule**, in the **Run** drop-down list, select when the policy should run.

Note that the scheduling options only become active if you select **By schedule** in the **Run** drop-down list.

- 2 To add a schedule, click **Add Schedule**, and then click one of the following:

- | | | |
|------------------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Scheduled Time | 1 | In the Start box, specify the appropriate time. |
| | 2 | If you want the schedule to repeat, click No Repeat and then, in the Repeat Schedule dialog, specify the appropriate frequency. |
| Schedule Window | 1 | In the Start, End, and Duration boxes, specify the appropriate times. |
| | 2 | In the During window, check every box, specify the appropriate interval. |
| | 3 | If you want the schedule to repeat, click No Repeat and then, in the Repeat Schedule dialog, specify the appropriate frequency. |

Each schedule is added to the policy schedule list. Repeat this step to add as many schedules as you want.

- 3 In the **Time Zone** drop-down list, select the appropriate time zone:

Use agent time The times are specified without time zone information and are applied at the local time at each managed computer. The schedules run at different times depending on the time zones of the managed computers.

Use server time The times are specified with time zone information, where the time zone offset is that of the server's time zone where the policy is defined. The schedules run simultaneously irrespective of time zones and are compensated for daylight saving.

This option ensures that the schedules are always coordinated with the specified local time on the server where the policy is created.

Coordinate using UTC The times are specified with time zone information, where the time zone offset is 0. The schedules run simultaneously irrespective of time zones and are not affected by daylight saving.

- 4 (Optional) If you want to remove a schedule from the list, select the schedule, and then click **Delete**.
- 5 Click **Advanced** and then, in the **Advanced options** dialog box, make the appropriate changes:

Only perform check if Check the appropriate options.

Start/End dates The start date is the date that the policy takes effect. The policy must be enabled in the same way as any other policy. You can enable the policy at any time before or after the start date.

If you want the policy to be available for a limited period of time, set the appropriate end date. The policy is unavailable after this date, whether or not it is enabled.

The end date setting is optional. If no end date is specified, the policy is available indefinitely.

- 6 In the **Advanced options** dialog box, click **OK**.
- 7 Under **Extra schedule options**, check the appropriate options.

About automation policies

Automation policies are system-defined, or administrator-defined, sets of rules that govern the execution of automated actions. Examples of automated actions include running a report using the parameters that were obtained from the policy, sending an alert to the administrator, and executing a command or running a task on managed computers.

See [“About Symantec Management Platform policies”](#) on page 319.

See [“Managing automation policies”](#) on page 330.

See [“Key components of automation policies”](#) on page 328.

Automation policies may be run on a schedule or triggered by Notification Server messages. The policy determines when an action should start, and who or what should be notified of the results. Automation policies are run on the Notification Server computer, so are not concerned with agent-related activity on managed computers. However, some automation policies may be triggered by messages which are generated by agent activity.

Automation policies are not applied to resource targets, unlike the other types of Notification Server policies. They are Notification Server actions which are performed on the appropriate managed computers. Some actions, such as sending an email to the administrator containing a report or a data source as an HTML file, do not affect any managed computers.

Many of the solutions that work with Notification Server come with automation policies. These policies let Notification Server perform a variety of actions when defined conditions occur. Automation policies can be set on a single process starting on a computer. , Automation policies can also be set on complex scenarios, such as multiple processes across a wide range of computers. Each solution that defines automation policies specifies its own criteria for the type of conditions that lead to the actions being initiated.

For example, Inventory Solution uses data from the CMDB, and application metering uses the list of monitored processes. In this solution, however, there are common sets of actions that can be run automatically.

Key components of automation policies

See [“About automation policies”](#) on page 327.

Automation policies have the same key components.

Table 27-2 Key components of automation policies

Component	Description
Trigger	<p>Initiates the evaluation of an automation policy.</p> <p>Notification Server provides the following triggers:</p> <ul style="list-style-type: none"> ■ Schedule Any Notification Server schedule, such as a shared schedule or a specified custom schedule. You cannot use maintenance windows (which are defined on the managed computers) as automation policy triggers. ■ Message An internal Notification Server message. These are sent when events of interest occur. For example, a resource created, a resource discovered, a resource deleted, a new computer discovered, or a Notification Server service started.
Data Source	<p>Provides information that the automation policy uses after it has been triggered. The data source is typically a report or a query that returns a list of computers, along with information about the state of each computer and its current settings that are relevant to the policy. The report or query is run when the policy is triggered to ensure that the most recent data is extracted.</p> <p>The data source defines the managed computers that are targeted by the policy and the actions that are performed on them. An automation policy may also extract parameters from the data source and use them as input parameters for tasks or jobs.</p> <p>Notification Server provides the following data sources:</p> <ul style="list-style-type: none"> ■ Report ■ Raw SQL Query If you select this option, you need the Edit SQL Directly privilege to be able to edit the data source query and view the query results. See "System privileges" on page 423. ■ Resource Query ■ Message ■ None <p>Solutions may add additional data sources.</p>
Evaluation Rule	<p>Evaluates the data that is contained in the data source and determines whether or not an action needs to be performed.</p> <p>Notification Server provides the following evaluation rules:</p> <ul style="list-style-type: none"> ■ Run for non-empty data ■ Run for each record ■ Message processing ■ Run always

Table 27-2 Key components of automation policies (*continued*)

Component	Description
Action	Specifies the task or job that the policy runs. These are standard agent or server-side tasks. The action may include input parameters that are passed from the data source.

Managing automation policies

You can configure and manage the automation policies that you have available on Notification Server. You can create new policies, edit existing policies, turn a policy on or off when necessary, set the appropriate security on a policy, and delete a policy when it is no longer required.

See [“About automation policies”](#) on page 327.

To manage automation policies

- 1 In the Symantec Management Console, in the **Manage** menu, click **Automation Policies**.
- 2 On the **Automation Policies** page, select the appropriate tab:

Schedules	Manage automation policies that run on a defined schedule.
System Messages	Manage automation policies that run when a specific system message is received.

- 3 Do any of the following:

Import policy	To import a policy from other system, do the following: <ul style="list-style-type: none"> ■ On the toolbar, click Import. ■ In the Import Item dialog box, specify the XML file of the policy, and then click OK.
Create or modify a policy	See “Creating or modifying scheduled automation policies” on page 331. See “Creating or modifying message-based automation policies” on page 333.
Turn a policy on or off	In the left pane, select the automation policy that you want to turn on or off, and then click Turn on or Turn off , whichever is appropriate.
Delete a policy	In the left pane, select the automation policy that you want to delete, and then click Delete . You can delete any automation policies that you have created. You cannot delete any of the default automation policies that are supplied with Notification Server.

Set security on a policy	<p>In the left pane, select the automation policy that you want to set security on, and then click Actions > Security Role Manager.</p> <p>In the Security Role Manager, set the appropriate security.</p>
Perform other actions on a policy	<p>In the left pane, select the automation policy that you want to perform an action on, and then click Actions, and then click the appropriate option.</p> <p>The available actions are the same as those on the context menu.</p>
Test a policy	<p>In the left pane, select the automation policy that you want to test, and then in the right pane, click Test Automation Policy.</p> <p>You can use the automation policy test to check that all of the policy components are consistent, and that the input parameters are mapped properly. The test executes the policy, and the results of the action are displayed in the Job/Task log.</p>

Creating or modifying scheduled automation policies

Automation policies may use any Notification Server schedule, such as a shared schedule or a specified custom schedule. Maintenance windows (which are defined on the managed computers) cannot be used to schedule automation policies. When an automation policy is triggered, the appropriate actions are run immediately. You cannot schedule an automation policy to run at a later time after it has been triggered.

See [“About automation policies”](#) on page 327.

See [“Managing automation policies”](#) on page 330.

Note: This topic covers the default options that are supplied with Notification Server. Solutions may extend these options or add new ones. For more information, refer to the appropriate solution documentation.

To create or modify a scheduled automation policy

- 1 In the Symantec Management Console, in the **Manage** menu, click **Automation Policies**.
- 2 On the **Automation Policies** page, on the **Schedules** tab, do one of the following:

To create a new policy	<ol style="list-style-type: none">1 Click New Policy.2 In the Automation Policy Name dialog, type the new policy name, and then click OK.
------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

To modify an existing policy	In the left pane, select the appropriate policy.
------------------------------	--------------------------------------------------

3 (Optional) In the right pane, edit the policy name and description by clicking the appropriate fields and typing the new details.

4 In the **Schedule** drop-down list, select the schedule that you want to use.

At Date/Time Specify the schedule date, time, and repetition in the appropriate fields.

Shared Schedule In the **Select Shared Schedule** drop-down list, select the appropriate schedule.

See [“Managing shared schedules”](#) on page 93.

5 In the **Details** panel, under **Data Source**, specify the data source to use.

See [“Specifying the automation policy data source”](#) on page 334.

6 Under **Conditions**, in the **Evaluation Rule** drop-down list, select the appropriate evaluation rule:

Run for non-empty data Treats the data source table as a single unit. When the policy is triggered, the action is run only if the table contains one or more rows, and is run once only.

You need to use this option if the data source contains information in an HTML file rather than a table.

This option lets you target everything in a single column, such as a list of GUIDs. You cannot set dynamic parameters to distinguish targeted computers. If you want to do that, you must use the Run for each record option.

Run for each record Evaluates the data source table row by row, which lets you use fields per row as dynamic parameters for the specified actions. The action is run once for each row.

Run always Runs the specified actions without using a data source.

This option is available only when no data source is specified.

7 Under **Actions**, specify the task or job to run, and set any required input parameters.

See [“Specifying the automation policy action”](#) on page 336.

8 Click **Apply** to save the policy settings.

9 (Optional) If you want to ensure that all of the policy components are consistent and that the input parameters are mapped properly, click **Test Automation Policy**.

The test is an internal check only and does not affect any resources.

Creating or modifying message-based automation policies

Automation policies may use an internal Notification Server message as a trigger. The messages that are available for this purpose are predefined. These messages relate to Notification Server events such as resources being discovered, created, or deleted, new computers being discovered, or Notification Server services being started. Solutions may make additional solution-specific messages available. When an automation policy is triggered, the appropriate actions are run immediately. You cannot configure an automation policy to run at a later time after it has been triggered.

See “[About automation policies](#)” on page 327.

See “[Managing automation policies](#)” on page 330.

To create or modify a message-based automation policy

- 1 In the Symantec Management Console, on the **Manage** menu, click **Automation Policies**.
- 2 On the **Automation Policies** page, on the **System Messages** tab, do one of the following:

To create a new policy

- 1 Click **New Policy**.
- 2 In the **Automation Policy Name** dialog, type the new policy name, and then click **OK**.

To modify an existing policy In the left pane, select the appropriate policy.

- 3 (Optional) In the right pane, edit the policy name and description by clicking the appropriate fields and typing the new details.
- 4 In the **NS Message** drop-down list, select the message that you want to use.

Show all messages

Lets you view and select all system messages.

Note that the list also includes the system messages that are initially not intended for using in the policies.

Apply message filter

Lets you trigger the automation policy only if it receives a message that matches the rule(s) that you specify.

For more information about applying and configuring filters for the NS Messages, see the following knowledge base article:

<http://www.symantec.com/docs/DOC9381>

- 5 In the **Details** panel, under **Data Source**, specify the data source to use.

See “[Specifying the automation policy data source](#)” on page 334.

- 6 Under **Conditions**, in the **Evaluation Rule** drop-down list, select the appropriate evaluation rule:

Run for non-empty data Treats the data source table as a single unit. When the policy is triggered, the action is run only if the table contains one or more rows, and is run once only.

You need to use this option if the data source contains information in an HTML file rather than a table.

This option lets you target everything in a single column, such as a list of GUIDs. You cannot set dynamic parameters to distinguish targeted computers. If you want to do that, you must use the Run for each record option.

Run for each record Evaluates the data source table row by row, which lets you use fields per row as dynamic parameters for the specified actions. The action is run once for each row.

Message processing Evaluates the data source message text and uses the appropriate parameters in the specified actions.

This option is available only when a message data source is used.

Run always Runs the specified actions without using a data source.

This option is available only when no data source is specified.

- 7 Under **Actions**, specify the task or job to run, and set any required input parameters.
See [“Specifying the automation policy action”](#) on page 336.
- 8 Click **Save Changes** to save the policy settings.
- 9 (Optional) If you want to ensure that all of the policy components are consistent and that the input parameters are mapped properly, click **Test Automation Policy**.
The test is an internal check only and does not affect any resources.

Specifying the automation policy data source

The automation policy data source determines which computers to target and what actions to perform on them. An automation policy may extract parameters from the data source and use them as input parameters for tasks or jobs.

See [“Creating or modifying scheduled automation policies”](#) on page 331.

See [“Creating or modifying message-based automation policies”](#) on page 333.

You can use external data sources such as reports and messages, or you can use a query to extract data from the CMDB. An external data source such as a report may be used by any

number of automation policies. You need to be careful when using reports, because they might be modified later and the parameters that some actions depend on could be changed or removed. If an action cannot determine a required parameter from a data source report, it uses the default value that is set in the automation policy.

See [“Creating and modifying custom Notification Server reports”](#) on page 378.

SQL queries and resource queries are embedded in the automation policy definition. You cannot share queries between automation policies, and you cannot directly access the queries (also known as data sources) that are components of reports. If you want to use a report query, you can copy the SQL from the report and paste it into the automation policy.

An automation policy that does not define a target for its action does not require a data source. For example, a policy that sends a message to the administrator, or performs a task on the Notification Server computer.

To specify the automation policy data source

- 1 In the Symantec Management Console, on the **Manage** menu, click **Automation Policies**.
- 2 On the **Automation Policies** page, on the **System Messages** tab, either select an existing automation policy or create a new one.
- 3 In the right pane under **Details**, under **Data Source**, in the **Data Source** drop-down list, select the appropriate option:

Report	Use the results of a report. <ol style="list-style-type: none">1 In the Report field, click Report Name.2 In the Select Report window, select the appropriate report, and then click OK.
--------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Raw SQL Query	Use the results of an SQL query. <ol style="list-style-type: none">1 Click Edit Query.2 In the Data Source window, specify the SQL query that you want to use, and then click OK.
---------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

See [“Defining an SQL query for a filter”](#) on page 307.

If you want to reuse a query from an existing filter or report, you can copy the content of the Resolved Query tab from the appropriate filter or report query. You can then paste it into the **Resolved Query** tab in the **Data Source** window. You can then modify the SQL as necessary.

Note that the query in the **Resolved Query** tab has any parameters replaced by the specified test values.

Resource Query	Use the results of a resource query. <ol style="list-style-type: none">1 Click Edit Query.2 In the Data Source window, specify the resource query that you want to use, and then click OK. See “Defining a resource query for a filter” on page 306.
Message	Use the information that is contained in the message that triggered the policy.
None	No data source is required. The automation policy does not need to define a target for its action.

Specifying the automation policy action

Automation policy actions are jobs and tasks. Symantec Management Platform supplies a set of tasks that you can use, and solutions may add more. You can create your own tasks and extend the options to suit your requirements. If your Symantec Management Platform is part of a hierarchy, further tasks and jobs may be replicated down from the parent Symantec Management Platform.

See [“Creating or modifying scheduled automation policies”](#) on page 331.

See [“Creating or modifying message-based automation policies”](#) on page 333.

An automation policy may contain only one action, which may be a task or a job, that is applied to all the computers that the policy targets. If you want to include multiple tasks, you need put them into a suitable job. Alternatively you need to create multiple automation policies with the appropriate triggers, data sources, and actions.

Warning: Any number of automation policies may share a job or task. When you modify a task that you want to use in an automation policy, your changes can affect many other policies. You may prefer to clone the relevant task and use the modified clone in the policy.

Tasks may contain both static input parameters and dynamic input parameters. Dynamic parameters are set with values extracted from the data source when the policy is triggered. Static parameters have values set within the task, so are the same every time that the task runs.

Failure actions or return codes cannot be set in an automation policy, so if any are needed, you must configure them in the task.

To specify the automation policy action

- 1 In the Symantec Management Console, on the **Manage** menu, click **Automation Policies**.
- 2 On the **Automation Policies** page, on the **System Messages** tab, either select an existing automation policy or create a new one.
- 3 In the right pane, under **Actions**, in the **Run job/task** field, click **Select a Job or Task**.
- 4 In the **Select Task** dialog box, in the left pane, select the appropriate job or task, then in the right pane, make any necessary configuration changes to the job or task, and then click **OK**.

Note that you can add an attachment to the automation policy e-mail. For example, you can use this option for **Send automated report e-mail** task or **Send automation policy e-mail** task.

For more information about adding an attachment to the automation policy email, see the following article:

[How to send attachment in the Automation Policy e-mail?](#)

- 5 (Optional) Click **Edit Input Parameter** and then, in the **Edit Job/Task Input Parameters** dialog box, specify the following for each action parameter:

Data Source	The data source field that supplies the parameter. Select the appropriate option from the drop-down list: <ul style="list-style-type: none">■ Results as HTML■ Results as CSV■ Results as text■ Number of rows■ Custom
-------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Custom Value	The value that is used when the data source is set to Custom. This value is the default that is used if the specified data source field is not available.
--------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------

This field is not shown if no input parameters are required.

- 6 (Optional) Click **OK** to close the **Edit Job/Task Input Parameters** window.
- 7 Click **Save Changes**.

Creating and modifying automation policy tasks

A set of automation policy tasks is provided with Symantec Management Platform. You can use them in your automation policies, and use them as a template for creating your own custom tasks and jobs.

See [“Specifying the automation policy action”](#) on page 336.

The tasks let you perform the following actions:

Assign to organizational group	Lets you assign resources to an organizational group.
Email a report	Lets you email a specified report. The emails are sent as plain text or with HTML. You may want to use this task as part of a job that also includes a run a report task to create the appropriate report.
Send an email	Lets you send an email with information you define to specified users. The email can include status, product license, or other information.
Run a report	You may want to use this task as part of a job that also includes an email a report task to send the report to the appropriate users or Notification Server administrator

To create or modify an automation policy task

- 1 In the Symantec Management Console, in the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, expand the **Jobs and Tasks > System Jobs and Tasks > Notification Server > Automation Policy Tasks** folder and then do one of the following:
 - To create a new job or task from scratch
 - 1 Right-click the **Automation Policy Tasks** folder, click **New**, and then click the appropriate option.
 - 2 In the **Create New Task** dialog box, in the left pane, select the task.
 - 3 In the right pane, specify the options, and then click **OK**.
 - To create a new job or task using an existing job or task as a template Right-click the job or task, and then click **Clone**.
 - To modify an existing job or task Click the job or task.
- 3 In the right pane, specify the appropriate details for the job or task.
- 4 Click **Save changes**.

Disabling or limiting Notification Server Event processing for a client computer

A Notification Server Event (NSE) is an XML file that is passed between Notification Server and the Symantec Management Agent (including solution plug-ins).

To disable or limit Notification Server Event processing for a client computer

- 1 In the Symantec Management Console, on the **Manage** menu, click **Filters**.
- 2 In the left pane, click **Computer Filters**, and then click one of the following filters:

Filter	Functionality
Blacklisted Host Computers	When you add a client computer to this filter, the NSEs related to a given client computer are put on hold.
User Configuration Blacklisted Users and Computers	When you add a client computer to this filter, the NSEs related to given user are put on hold.

- 3 In the right pane, click **Edit**, and then add the needed targets to the filter.
- 4 Click **Save changes**.

Using tasks and jobs

This chapter includes the following topics:

- [About Task Management](#)
- [Task Management components](#)
- [How task server uses the tickle mechanism](#)
- [When to use tasks, jobs, and policies](#)
- [About running tasks in hierarchy](#)
- [Sequencing tasks](#)
- [Viewing and editing permissions on a task type](#)
- [Creating tasks to input or to output task properties](#)
- [Cleaning up task data](#)
- [Cleaning up task schedules](#)
- [Cleaning up task version data](#)
- [Changing Client Task Agent settings](#)

About Task Management

Task Management provides task sequencing and automation for Symantec solutions. Task sequencing lets you perform complex management operations in a single job. Tasks can be sequenced in a job, which gives you great flexibility in your work. The functionality is similar to what Symantec Deployment Solution software provides with its job engine. However, Task Management is built on the Symantec Management Platform and lets the rest of the Symantec solution catalog take advantage of its powerful features.

See [“Sequencing tasks”](#) on page 347.

You can run tasks automatically based on events in the system or changes in the database. You can also run tasks automatically to keep computers compliant with policies.

Task servers are similar to package servers in that they are designed to reside on a separate server and are very lightweight. Both task servers and package servers are site services and install on a site server. Computers can be assigned to a specific site server by either computer name or by subnet.

See [“About site services”](#) on page 97.

You can create, run, or schedule jobs and tasks from the Jobs and Tasks portal. Task components orchestrate these jobs and tasks smoothly.

See [“Task Management components”](#) on page 341.

Task Management includes the following features:

- Executes multiple tasks in a defined sequence that is called a job.
See [“Creating a job”](#) on page 350.
- Lets the users provide logic to handle task errors or other return codes.
- Includes the powerful command line and VBscript capabilities.
- Provides the predefined power management tasks.
- Executes the client-side and server-side tasks.
See [“Deploying a task server”](#) on page 348.
- Provides the quick acting features for running jobs, such as Run Now options and near real-time status feedback.
See [“Running a job or task”](#) on page 352.
See [“Adding a schedule to a policy, task, or job”](#) on page 354.
See [“Viewing the task status on the Symantec Management Agent”](#) on page 355.
- Reuses the tasks in multiple jobs or lets you clone and modify tasks as wanted.

Task Management components

Task Management works by leveraging several components. These components orchestrate the assignment and performance of tasks and jobs on the connected client computers.

See [“About Task Management ”](#) on page 340.

Table 28-1 Task Management components

Component	Description
Task Server	<p>This component distributes jobs and tasks on the network and it can be run on Notification Server or on a remote computer.</p> <p>The task server has the ability to tickle the registered client computers. This tickle ability is separate from the tickle server component on the Notification Server computer. The task server sends the status information to the Data Loader. It also sends the tickles, the job, and the task information to the Client Task Agent.</p>
Tickle Server	<p>The tickle server notifies the task server when and where there are tasks to run on its connected client computers. The tickle server then tickles those connected client computers and sends them the XML that contains the job or the task information using HTTP(S). The tickle server also collects status information and forwards it to the Configuration Management Database (CMDB) using HTTP(S).</p> <p>This component runs only on the Notification Server computer. It sends an IP tickle packet to task servers when any of their clients have a job or task to run.</p> <p>See “How task server uses the tickle mechanism” on page 343.</p>
Data Loader	<p>This component receives status information from task servers and caches it in memory until it can be sent to the CMDB. The data loader improves scalability by allowing status information for several hundred clients to be received at the same time without overwhelming the SQL Server.</p> <p>This component also runs on each remote task server and queues up the data that waits until it can be sent to Notification Server.</p>
Client Task Agent	<p>This agent runs on client computers and performs the following actions:</p> <ul style="list-style-type: none"> ■ Accepts tickles from a task server. ■ Receives the job and the task information. ■ Passes the information to a handler. ■ Sends the status information back to the task server. <p>This agent is installed automatically with the Symantec Management Agent.</p> <p>Note: When you install the Symantec Management Agent on a computer, there is a delay before the Client Task Agent registers with Notification Server. Any tasks that are targeted at the computer during this time (typically about 10 minutes) have a pending status until the Client Task Agent registers. When the Client Task Agent is registered, the tasks are executed immediately.</p>

How task server uses the tickle mechanism

The tickle server is a component of Task Management. The tickle server component runs only on the Notification Server computer and is responsible for notifying task servers of pending tasks for their client computers. Tickle connection between Notification Server and task servers is also used for delivering new task server settings to task servers.

Task servers have the native ability to tickle their registered client computers. This tickle ability is separate from the tickle server component on the Notification Server computer.

See [“Task Management components”](#) on page 341.

The tickle server sends IP tickle packets to task servers when any of their registered client computers have a job or task to run. After the tickle packet is received, the task server immediately requests the task or the job information from Notification Server for its registered client computers. It also tickles its client computers. When the Client Task Agent receives the tickle packet, it requests the job or the task information from its registered task server. Only after the Client Task Agent receives the task information is the task executed. Status events for completed tasks are sent back to the registered task server upon completion.

If the tickle packets are blocked or otherwise cannot reach the destination, the Client Task Agent automatically checks back to its registered task server for any new job information. It performs this check every 30 minutes. This Task Request Interval is configurable in the Symantec Management Console. Task Server task and job information is not received through the Symantec Management Agent configuration policy. It is received directly by the Client Task Agent from its registered task server. If you force the Symantec Management Agent to update its configuration policy, it does not force the Client Task Agent to receive pending task information.

See [“Changing Client Task Agent settings”](#) on page 360.

By default, the Tickle Server uses port 50123 for task servers and task servers use port 50124 to tickle Client Task Agents.

Note: Tickle mechanism does not function in Cloud-enabled Management (CEM) mode.

See [“About Task Management ”](#) on page 340.

The following example assumes the Client Task Agent for ComputerA is registered with RemoteTaskServer1.

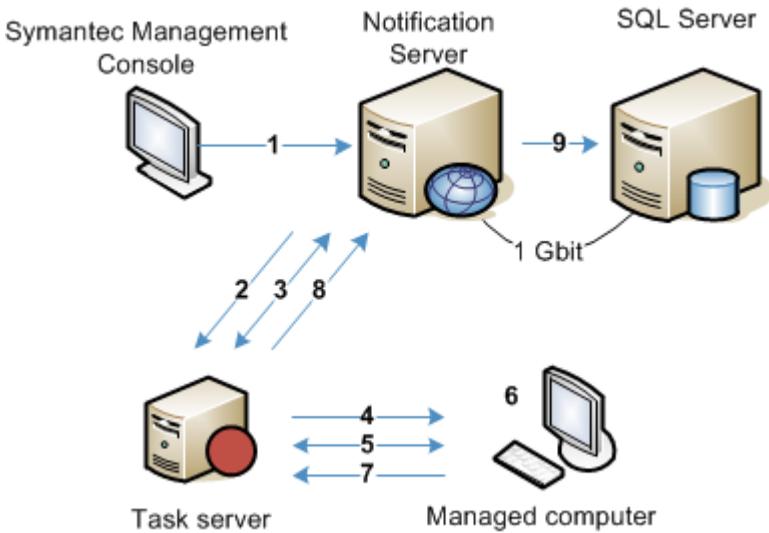
Table 28-2 Sequence for how the task server tickle works

Sequence	Description
One	A Notification Server administrator assigns a task to run immediately on ComputerA.

Table 28-2 Sequence for how the task server tickle works (*continued*)

Sequence	Description
Two	The Tickle Server on the Notification Server computer sends a tickle packet to notify RemoteTaskServer1 of the pending task.
Three	RemoteTaskServer1 receives the tickle packet and immediately requests the job information from Notification Server.
Four	RemoteTaskServer1 tickles ComputerA to notify it of the pending task.
Five	ComputerA receives the tickle packet and immediately requests the job information from its registered task server – RemoteTaskServer1.
Six	ComputerA receives the job information and executes the task.
Seven	Upon completion of the task, ComputerA sends a status event back to RemoteTaskServer1.
Eight	RemoteTaskServer1 caches the status event and immediately attempts to forward it back to Notification Server.
Nine	Notification Server receives the status event from RemoteTaskServer1 and records the information in the database.

Figure 28-1 Sequence for how task server tickle works



When to use tasks, jobs, and policies

Tasks, jobs, and policies have different uses in Notification Server. Which one you use depends on what you want to accomplish.

A policy is a set of rules that apply to a resource or set of resources (known as the policy target). A policy may be evaluated based on a schedule or based on incoming data. When a policy is evaluated, the appropriate action is taken. This action typically includes running tasks on the target resources to ensure that they all comply with the policy. Using a policy lets you apply actions to particular resources, which you define as the policy target.

See [“About Symantec Management Platform policies”](#) on page 319.

A task is a separate action which does not have ongoing actions and which you deploy to selected computers. You can run tasks automatically based on events in the system or changes in the database. You can also run tasks automatically to keep computers compliant with policies.

A job is a sequence of tasks which are run in a specific order.

See [“About Task Management”](#) on page 340.

In general use policies for ongoing management; and use tasks to enforce policies or perform one-time actions.

Table 28-3 When to use tasks, jobs, and policies

Option	Criteria
Task	Use a task when the following criteria is true: <ul style="list-style-type: none"> ■ You need to perform an action that finishes quickly (no ongoing actions).
Job	Use a job when the following criteria is true: <ul style="list-style-type: none"> ■ You need to run actions in a specific order. ■ An action can be useful for a user to sequence or tie to a Notification Server message.
Policy	Use a policy when the following criteria is true: <ul style="list-style-type: none"> ■ You have static configuration data to send to the Symantec Management Agent. ■ You have ongoing actions with no definite end.

About running tasks in hierarchy

Symantec Management Platform lets you create tasks on parent Notification Server and run them on all client computers in the hierarchy. Such tasks are also replicated to the child Notification Server and they run on all the applicable managed computers.

See [“About Notification Server hierarchy”](#) on page 127.

See “[About Task Management](#)” on page 340.

When you run tasks in hierarchy, you must consider the following design specifics:

Client computers report task status information only to Notification Server to which they are assigned. The task status information for the client computers that are assigned to a child Notification Server is not displayed on parent Notification Server.

If you create a task on parent Notification Server and run it on all client computers in your environment, not all computers report back to the parent Notification Server. The client computers that are assigned to the child Notification Server report the task status information only to the child Notification Server. Also, the task status information is not replicated from the child Notification Server up to its parent.

Therefore, the **Jobs / Tasks** page on parent Notification Server does not display the task status information for the tasks that run on the client computers assigned to a child Notification Server. The progress bar of these tasks is gray on the parent Notification Server.

You can see the accurate task status information for each computer separately on the parent Notification Server, in the **Task Instance Details** window. Note that the **Task Instance Details** window opens a URL of the child Notification Server and requires the credentials of the child Notification Server.

Note that if you replicate the task to the child Notification Server and launch the task from there, you cannot view the task status details on parent Notification Server. The status of this task is displayed as **Replicated** on the parent Notification Server.

The server job that contains client tasks is not properly replicated from parent Notification Server to its child.

If you create a server job that contains client tasks and replicate it from a parent Notification Server to its child, the client tasks within the server job replicate down to the child Notification Server but the server tasks and the server job itself does not. Additionally, server tasks from that particular job run on the parent Notification Server while client tasks run on the child Notification Server.

To work around this issue, you can create a server job on the child Notification Server and add the replicated client tasks to it. Alternatively, you can create a client job on the parent. The client job that contains client tasks is properly replicated down.

If you apply a server job that contains client tasks from parent Notification Server to the child Notification Server, the job run status is available only on the parent Notification Server. On the child Notification Server, the instance of that particular job is not created.

Note that Symantec does not recommend creating a server job that contains client tasks.

For more information about jobs and tasks, see the following knowledge base article:

<http://www.symantec.com/docs/HOWTO9671>

If you delete the task on parent Notification Server, the **Replicate now** option does not delete this task on child Notification Server.

For jobs containing only server tasks and for server tasks, the schedule is not replicated from parent to child Notification Server.

If you delete a task on parent Notification Server and use **Replicate now** option to replicate this operation to child Notification Server, the task on child Notification Server is not deleted.

Only differential or full replication deletes the task successfully on child Notification Server.

If you create and schedule a new server task on the parent Notification Server and then replicate it to child Notification Server, the schedule is not replicated to the child. You have to schedule this task separately on the child Notification Server.

Sequencing tasks

Task sequencing lets you perform complex management operations in a single job. Tasks can be sequenced in a job, which gives you great flexibility in your work.

See [“About Task Management”](#) on page 340.

Table 28-4 Process for sequencing tasks

Step	Action	Description
Step 1	(Optional) Deploy a task server.	<p>Task servers let you distribute jobs and tasks to client computers on your network.</p> <p>Symantec recommends deploying at least one task server per Notification Server. After deploying the initial dedicated task server, add additional task servers for every 5000 to 7500 client computers. The number of the managed computers that a task server can serve depends on the hardware of the task server computer.</p> <p>See “Deploying a task server” on page 348.</p>
Step 2	(Optional) Configure a Task Server communication profile.	<p>By default, Task Server uses the predefined Symantec Management Agent communication profile to communicate with Notification Server. To change the default settings, you must configure a Task Server communication profile and apply it to required Task Servers using the Task Service Settings.</p> <p>See “Configuring a Task Server communication profile” on page 349.</p>
Step 3	Create a task.	<p>Tasks that are run on Notification Server or managed computers.</p> <p>See “Creating a task” on page 350.</p>

Table 28-4 Process for sequencing tasks (*continued*)

Step	Action	Description
Step 4	Create a job.	Jobs run tasks, other jobs, and conditions. See “Creating a job” on page 350.
Step 5	Run jobs or tasks.	Jobs and tasks can be run on Notification Server or managed computers. See “Running a job or task” on page 352. See “Rerunning a failed task” on page 352. See “Adding a schedule to a policy, task, or job” on page 354.
Step 6	View real-time status of the jobs or tasks.	You can view the status of the job or task in the Symantec Management Console and also on a client computer, on the Symantec Management Agent. Note: For improved performance, in the Symantec Management Console, the task status is updated every five minutes. See “Viewing the task status on the Symantec Management Agent” on page 355.

Deploying a task server

Task servers let you distribute your jobs and tasks to different computers on your network where Symantec Management Agents can run the jobs and tasks. When you distribute jobs and tasks, you reduce the network traffic and the load on Notification Server. The Symantec Management Agent accesses the closest task server for job and task downloads.

See [“Task Management components”](#) on page 341.

Each Notification Server becomes a task server when the Task Server component is installed. You can then deploy more task servers as needed.

The requirements for a task server computer are as follows:

- Supported operating system
[Platform Support Matrix](#)
- Microsoft Internet Information Services (IIS)
- .NET Framework (one of the versions from 4.5.1 to 4.7)
- Symantec Management Agent

Symantec recommends that you deploy task servers using site services. You can also manually deploy task servers.

If you deploy the task server manually, use the following example to specify the command line for the task server MSI to create the site server definition on Notification Server:

```
TaskServerSetup_x64.exe -a /ALL:a /qb REBOOT=ReallySupress /a  
NSURL="http://MYNS.mydomain.com/Altiris/" /s true /r false
```

See [“About site services”](#) on page 97.

This task is a step in the process for sequencing tasks.

See [“Sequencing tasks”](#) on page 347.

To deploy a task server using site services

- ◆ Deploy a task server as a site server.
 - See [“Managing site servers”](#) on page 106.

Configuring a Task Server communication profile

A Task Server communication profile lets you configure how Task Server communicates with Notification Server.

By default, Task Server uses the predefined Symantec Management Agent communication profile to connect to Notification Server. To change the default settings, you must configure a Task Server communication profile and apply it to required Task Servers using the **Task Service Settings**.

Note: A Task Server communication profile replaces the **Preferred Host** advanced option on the **Task Service Settings** page. If you have specified the **Preferred Host** for your Task Servers before the upgrade, a Task Server communication profile is automatically created during the upgrade to IT Management Suite 8.5.

To create a Task Server communication profile

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Agents/Plug-ins > Symantec Management Agent > Symantec Management Agent Communication profiles**, right-click the **Task Server Communication profiles** folder, and then click **New Profile**.
- 3 On the communication profile page, make the necessary changes.

For more information, click the page and then press **F1**.

- 4 Turn on the policy.

At the upper right of the page, click the colored circle, and then click **On**.

- 5 Click **Save changes**.

Note that you apply the Task Server communication profile to a Task Server using **Task Service Settings**.

Creating a task

You create and deploy tasks to managed computers using predefined task types. The type of task you choose depends on what you want to accomplish. Many types of tasks are provided with Task Management. Some Symantec solutions also provide task types and sample jobs.

This task is a step in the process for sequencing tasks.

See [“Sequencing tasks”](#) on page 347.

To create a task

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, right-click the folder where you want to create the task, and then click **New > Task**.
- 3 In the **Create New Task** dialog box, in the left pane, select the task type.
- 4 In the right pane, configure the task.
- 5 (Optional) To specify the timeout period for the task and the user account under which this task should run on the client computer, click **Advanced**.

Note that these options are only available for some type of tasks.

- 6 Click **OK**.

Creating a job

You can create jobs that run multiple tasks or jobs. The two types of jobs are server jobs and client jobs. Server jobs run on Notification Server. Client jobs are deployed to managed computers by a task server. The managed computer then runs the job and reports back to Notification Server.

Jobs can contain multiple tasks, multiple jobs, and multiple conditions, which gives you great flexibility in setting up the job sequence that you need.

This task is a step in the process for sequencing tasks.

See [“Sequencing tasks”](#) on page 347.

To create a job

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, right-click the folder where you want to create the job, and then click **New > Server Job** or **New > Client Job**.
- 3 In the right pane, under **Jobs / Tasks**, configure the job:

Edit the name of the job Click the name text and type the new name.

- Create a new task to add to a job
- 1 Click **New > Task**.
 - 2 In the **Create New Task** dialog box, in the left pane, select a task.
 - 3 In the right pane, configure the task.
 - 4 Click **OK**.

- Add an existing task or job to a job
- 1 Click **Add Existing**.
 - 2 In the **Add Existing Task** dialog box, in the left pane, you can search for the tasks or jobs, and then select multiple tasks or jobs to be added simultaneously.
 - 3 Click **OK**.
- You can use the up and down arrows on the menu to move tasks, jobs, and conditions.

- Add a condition to a job
- 1 Click **New > Condition**.
 - 2 In the **Edit Condition** dialog box, the rule gives a **Where** clause that lets you select a task or job, an operation to perform, and a condition for performing the operation on the task or job.
 - 3 In the first drop-down list, select or enter the task or job and the return code for the condition.
 - 4 In the second drop-down list, select the operation for the rule to perform.
 - 5 In the third field, enter the condition.
 - 6 (Optional) To add more rules, click **Add Rule**.
 - 7 Click **OK**.

You can add one or more tasks or jobs to run as a result of the condition under **Else**.

- 1 Specify the timeout period for the job.
- 1 Click **Advanced**.
- 2 In the **Task options** dialog box, specify the timeout period for the job, and then click **OK**.

- 4 Click **Save changes**.

Running a job or task

The jobs and tasks that you create can be run on Notification Server or on managed computers depending on whether they are server tasks or client tasks. Server tasks are the tasks that run on a Notification Server computer. Client tasks are the tasks that run on a client computer.

If more than one task is added to a job, they are performed one after another. If a condition is added, the tasks that are performed are based on the results of the condition. The server must receive status of a previous task that has completed before it starts the next task in the job. There might be a delay of a few seconds before the next task begins.

This task is a step in the process for sequencing tasks.

See [“Sequencing tasks”](#) on page 347.

To run a job or task

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, select the job or task that you want to run.
- 3 Add a schedule to run the job or task.

See [“Adding a schedule to a policy, task, or job”](#) on page 354.

Rerunning a failed task

You can rerun a task against failed computer(s).

See [“About Task Management”](#) on page 340.

The task rerun works as follows:

- You can select multiple task instances to rerun. All failed computers from the included task instances are included in the rerun task instance.
- You can rerun only failed client tasks, not failed server tasks.
- **Rerun failed** ignores any target that was used in the previous task instance no matter how it was created (Quick Run, Schedule against a computer list, or schedule against a Target). It reruns against the list of failed computers from the task you just ran.

Note: Use the rerun task function only at the child Notification Server level, where you can see task status indicators. Symantec recommends that you do not rerun tasks from a parent Notification Server in a hierarchy because of time delays in replicating the data.

To rerun a failed task

- 1 In the Symantec Management Console, on the **Manage** menu, click **Computers**.

Note: You can also go directly to **Manage > Jobs and Tasks** and skip steps 2 and 3.

- 2 Click the double arrows (>>) at the top of the list pane to navigate to the **Software Deliveries** container summary.
- 3 Under **Quick Delivery Tasks**, click a task instance that failed on some of the computers and that you want to rerun on those computers.
- 4 In the **Task Status** pane, click **Rerun failed** to rerun the task instance(s) on the list of computers that returned a **Failed** status.
- 5 This action launches the **New Schedule** window. It pre-populates the **Selected Devices** field with the computers where the task instance(s) failed to run.

Note: If you click **Rerun failed** on a task instance with no failed computers, a pop-up message indicates that there are no failed computers with this task instance. When you click **Rerun failed** on a task instance that is in a pending or running state, no computers are listed, because the task has neither succeeded nor failed yet.

- 6 Click **Schedule** to schedule the task to rerun on the failed computers.

This creates a new instance of the task. The old instance is still there.

Note: You might encounter an error message that reads: “This task run has been deleted and cannot be viewed or rerun. Only summary data exists”. Task Management has a daily cleanup task that runs per user specifications to limit the number of working rows in the database. This prevents Task Management performance from slowing down too much. By default, every night, the cleanup task retains only the 200,000 most recent task instances. The computer count still shows all the computers that the task was run against. However, if the details of any of those task instances have been deleted, the **Rerun failed** does not include those tasks. As a result, there might be a discrepancy between the computer count where the task failed and the count when you click **Rerun Failed**.

- 7 This new schedule will now show up in the **Software Deliveries** flipbook page. You can view which instance of the task ran or reran most recently. You can also see how many computers the task was successfully or unsuccessfully run on.

Adding a schedule to a policy, task, or job

When you schedule a policy, task, or job to run, you have two options: quick run and schedule. The quick run option runs the current policy, task, or job immediately on a computer you specify. The schedule option provides several scheduling and target computer options. The schedule option lets you set a schedule. The target must be defined elsewhere.

To add a quick run schedule

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, select the policy, job, or task to which you want to apply the quick run.
- 3 In the right pane under **Task Status**, click **Quick Run**.
- 4 In the **Quick Run Now** dialog box, select the name of the computer on which you want to run the policy, task, or job.
- 5 Click **Run**.

To add a new schedule

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, select the policy, job, or task that you want to schedule.
- 3 In the right pane under **Task Status**, click **New Schedule**.
- 4 In the **New Schedule** dialog box, configure the schedule.

- 5 Click **Schedule**.

When tasks or jobs are selected to run, they appear in the Job and Task Status section.

Viewing the task status on the Symantec Management Agent

The task status (including the task history) is registered on the Symantec Management Agent. To view the task status on a computer, open the Symantec Management Agent. The task status lets you see which tasks have run and the result.

This task is a step in the process for sequencing tasks.

See [“Sequencing tasks”](#) on page 347.

To view task status on the Symantec Management Agent

- 1 On the computer that you want to view the status, double-click the icon on the system tray to open the Symantec Management Agent.
- 2 In the **Symantec Management Agent** window, click the **Task Status** tab.

Viewing and editing permissions on a task type

You can view and edit the permissions on task type properties. Changing permissions on the task type enables you to control which users can create new tasks. Users who have the Create New Task permission can create new tasks of that type.

See [“About Task Management ”](#) on page 340.

See [“Sequencing tasks”](#) on page 347.

See [“Security permission categories”](#) on page 420.

See [“Task Server permissions”](#) on page 435.

To view and edit permissions on a task type

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, click **Notification Server > Task Settings > Task Types**.
- 3 Navigate to the task type that you want to view, and then click it.
- 4 In the right pane, click **View permissions**.
- 5 To edit permissions, in the Security Role Manager, edit permissions on the task type.
See [“Assigning security permissions to folders and items”](#) on page 78.

Creating tasks to input or to output task properties

Input properties are the properties that are passed into a task from some source. Tasks can receive input properties from a set value, from other tasks, or at run time. Tasks can use these input properties (similar to variables) to perform their functions. All properties that are available to a task (both input properties and properties that the task creates) are called task properties.

A task can output its task properties to other tasks. If you have a task that outputs properties, any subsequent task in that job can use those output properties for its input properties. The tasks do not need to be concurrent.

You do not need an output task for each input task. Input tasks can also receive input from a set value or at run time.

See [“About Task Management”](#) on page 340.

See [“Creating a task”](#) on page 350.

To create a task that outputs properties

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, right-click the folder where you want to create the task, and then click **New > Task**.
- 3 In the **Create New Task** dialog box, in the left pane, select the task that has an **Advanced** option (for example: **Run Script**).
- 4 In the right pane, click **Advanced**.
- 5 Check **Save script output with task status**, and then click **OK**.

When this box is checked for a task, all of its task properties become viewable and available to subsequent tasks in a job.

- 6 Configure the task.
- 7 In the **Create New Task** dialog box, click **OK**.

To create a task that gets input properties from another task

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, right-click the folder where you want to create the task, and then click **New > Task**.
- 3 In the **Create New Task** dialog box, in the left pane, select a script task.
Script tasks receive input properties.
- 4 To use this task to pass the properties to another task, click **Advanced**, check **Save script output with task status**, and then click **OK**.

- 5 In the **Create New Task** dialog box, in the script command section, enter one or more tokens (for example: `%!input!%`) that catch the output.
- 6 Click **OK**.

To set up tasks within a job for input

- 1 Create a job and place in it the tasks that you created for output and input. Each output task must precede the task that receives its output.

See “[Creating a job](#)” on page 350.

- 2 Configure each input task in the job.

A task input appears on the right side when you click on the task in the following situations: when a client task has input and is in a client job, or when there is a client task inside of a server job.

Prompt me for task input each time this job is run Select to enter the input manually when the job runs.

Enter task input now

Select to enter the task input at this time:

- **Use a set value**
Select to use a value that doesn't change. Enter the value in the field that appears when the screen refreshes. If this task is a client task inside a server job, you must select the computer or computers that runs the client task. All client tasks have this parameter as a default input parameter when they are inside server jobs.
- **Use a previous task's output**
Select to use a previous task's output. Use this parameter if there is an output task in this job you want to use. When the screen refreshes, the variable name appears as well as a list of available output tasks. Select the task whose output you want to use for this task.
- **Prompt at run time**
Select to be prompted for the input at run time.

- 3 Click **OK**.

Cleaning up task data

To decrease the load on your system resources, task data can be archived or deleted using cleanup options.

See “[About Task Management](#)” on page 340.

See [“Sequencing tasks”](#) on page 347.

To clean up task data

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, click **Notification Server > Task Settings > Clean up Task Data**.
- 3 On the **Clean up Task Data** page, edit the required details.

Every night, the current task data and archived task data gets moved or deleted according to the following settings.

Maximum number of working database rows

After the number of working database rows reaches the maximum number, the oldest rows get archived until the maximum number is no longer exceeded.

Working database rows are the database rows that have been used recently. Symantec recommends that you keep this number small to decrease the load on your system resources.

Minimum time period to keep the task instances/summaries

Lets you specify the minimum time period for which you want to keep the task instance summaries in the database.

In the environment with high task load, the **Cleanup Task Data** task may remove the task instances of the recently executed tasks. As a result, some task instances might be missing and the summary information for that task may be incorrect.

To avoid this problem, enable the **Minimum time period to keep the task instances/summaries** option. If you enable this option, the **Clean-up Task Data** task does not remove the task records that are newer than the defined time period.

Note: The **Minimum time period to keep task instances/summaries** option overrides the **Maximum number of working database/database summary rows** option.

For example, if you set **Minimum time period to keep the task instances/summaries** to **1 Month** the clean-up does not remove the task records if they are newer than one month even if the **Maximum number of working database/database summary rows** is exceeded.

Run Cleanup Task on demand

If you select this option and if the number of used rows is exceeded, the cleanup task is started immediately.

- 4 (Optional) Add a schedule to clean up the task data.

See [“Adding a schedule to a policy, task, or job”](#) on page 354.

- 5 Click **Save changes**.

Cleaning up task schedules

When a task or a job is scheduled to run in the future, a task schedule is created in the Configuration Management Database (CMDB) and a scheduled task is created in the Windows Task Scheduler. The task will run at the specified time.

After the task runs, the task schedule remains in the CMDB and the scheduled task in the Windows Task Scheduler even if it has no future occurrence. The growing number of scheduled tasks can cause performance issues for Windows Task Scheduler.

The **Clean up Task Schedules** task lets you disable or delete the schedules that have no occurrence in the future.

Note: The existing schedules are re-saved during the upgrade. Running the **Clean up Task Schedules** task immediately after the upgrade does not disable or delete these schedules.

See [“About Task Management”](#) on page 340.

To clean up task schedules

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, click **Notification Server > Task Settings > Clean up Task Schedules**.
- 3 On the **Clean up Task Schedules** page, edit the options as follows:

Disable expired schedules with no occurrence during last This option lets you disable the task schedule in the CMDB and remove the scheduled task from Windows Task Scheduler.

Delete expired schedules with no occurrence during last This option lets you remove the task schedule from CMDB and scheduled task from Windows Task Scheduler.

Process only task schedules If you check this option, only the task schedules are disabled or deleted.

If you uncheck this option, all schedules that you have created in IT Management Suite are processed.

Note: The **Clean up Task Schedules** task deletes only task schedules. Other schedules are only disabled despite the configured settings.

- 4 (Optional) Add a schedule to clean up the task schedules.
See [“Adding a schedule to a policy, task, or job”](#) on page 354.
- 5 Click **Save changes**.

Cleaning up task version data

To decrease the load on your system resources, task version history can be archived or deleted using cleanup options.

See [“About Task Management ”](#) on page 340.

See [“Sequencing tasks”](#) on page 347.

To clean up task version data

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, click **Notification Server > Task Settings > Clean up Version Data**.
- 3 On the **Clean up Version Data** page, edit the required details.

By default, every week, task versions are deleted according to the following settings.

Maximum number of task versions to keep in the database

After the number of versions reaches the selected number, the oldest ones get deleted to improve database performance.

You can select to keep either 1, 5, 10 or 20 versions of a task in the database.

- 4 (Optional) Add a schedule to clean up the task data.
See [“Adding a schedule to a policy, task, or job”](#) on page 354.
- 5 Click **Save changes**.

Changing Client Task Agent settings

The Client Task Agent is part of the Symantec Management Agent. It receives jobs and tasks from the task server and runs them on managed computers. It then reports back to Notification Server.

Note: When you install the Symantec Management Agent on a computer, there is a delay before the Client Task Agent registers with Notification Server. Any tasks that are targeted at the computer during this time (typically about 10 minutes) have a pending status until the Client Task Agent registers. When the Client Task Agent is registered, the tasks are executed immediately.

Note: Usually the Client Task Agent opens a direct connection to Task Server on port 50124. Task Server uses this connection to tell the agent when new tasks are available. However, if a proxy is being used, a direct connection is impossible, so Task Server cannot tell the agent when new tasks become available. To keep up-to-date, you need to set the appropriate **Check Task Server for new tasks** value in the **Task Update** field.

See [“About Task Management”](#) on page 340.

See [“Sequencing tasks”](#) on page 347.

See [“Task Management components”](#) on page 341.

You can change Client Task Agent settings to improve the efficiency of work between the Client Task Agent and the Task Server. To improve efficiency, you can set the time interval that you want the Client Task Agent to request tasks from the Task Server. You can define the default method by which Notification Server selects a Task Server. You can also define the action you want to perform if multiple task servers are available at a site.

To change Client Task Agent settings

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, click **Notification Server > Task Settings > Task Agent Settings**.
- 3 On the **Task Agent Settings** page, edit the required details.

Check Task Server for new tasks every The interval, in minutes, that you want the agent to request tasks from the task server.

When multiple Task Servers are available at a site The action you want to perform if multiple task servers are available at a site.

- 4 Select the targets, computers, or users for the changes to apply to.
- 5 Click **Save changes**.

Using Resource Manager

This chapter includes the following topics:

- [About resource management](#)
- [Accessing Resource Manager](#)
- [Viewing inventory data for a data class](#)
- [Viewing event data for a data class](#)
- [Adding a resource to an organizational group](#)
- [Resource Manager tasks](#)

About resource management

You can manage the resources in the Configuration Management Database (CMDB) using the Resource Manager. Resource Manager lets you view information and perform numerous tasks on a resource. The information available and the tasks you can perform depend on the type of resource that is selected.

When you access Resource Manager, the **Base Resource Portal Page** is displayed for all resources except computers and software packages. For a computer resource or software package, the **Resource Manager** page displays. The page that displays for non-computer resources contains the **Item Property Summary** Web part. This Web part displays property information about the selected resource (such as GUID and product name). For a computer resource, the page displays a summary page for the computer resource. If you click **Resource Manager Portal** on the **Home** menu, you can access the **Item Property Summary** Web part for a computer resource.

See [“Resource Manager tasks”](#) on page 365.

You can access Resource Manager in several ways. The different methods make accessing Resource Manager easy, regardless of where you are in the Symantec Management Console.

See [“Accessing Resource Manager”](#) on page 363.

Accessing Resource Manager

You can access Resource Manager in the following ways:

- Using the **Manage** menu on the Symantec Management Console
- Right-clicking a resource in a list or report
- Double-clicking a resource in a list or report
- Typing a URL in your Web browser

See [“About resource management”](#) on page 362.

To access Resource Manager from the Manage menu

- 1 In the Symantec Management Console, on the **Manage** menu, click **Resource**.
- 2 In the **Select Resource** dialog box, select the resource you want to manage, and then click **OK**.

Resource Manager page opens with summary information about the selected resource.

To access Resource Manager from a right-click menu

- ◆ In a list of resources or a report within the Symantec Management Console, right-click the resource you want to manage and click **Resource Manager**.

In some lists, resources, or reports, the right-click option for Resource Manager might not be available. In these cases, use one of the other methods to access Resource Manager.

To access Resource Manager by double-clicking a resource

- ◆ In a list of resources or a report within the Symantec Management Console, double-click the resource you want to manage.

To access Resource Manager from a URL

- ◆ In a browser window, type the following URL:

```
http://NS Name/Altiris/Console/Dashboard/DashboardView.aspx?name=Target Resource Name
```

NS Name is the name of the Notification Server computer. *Target Resource Name* can be the resource name, the resource GUID, or the item GUID. If you omit “?name=*Target Resource Name*”, Resource Manager opens with the following error:

```
No resource GUID was supplied.
```

When using a case-sensitive database, ensure that the target resource name matches the name and case of the resource in the Configuration Management Database (CMDB).

Viewing inventory data for a data class

Using Resource Manager, you can view event data for a particular data class. The inventory data that is displayed depends on the data class selected. In general, you can view status and current data. When applicable, historical data is also available.

See [“Accessing Resource Manager”](#) on page 363.

To view inventory data for a data class

- 1 In the Symantec Management Console, on the **Manage** menu, click **Resource**.
- 2 In the **Select Resource** dialog box, select the resource you want to manage, and then click **OK**.
- 3 In **Resource Manager**, on the **View** menu, click **Inventory**.
- 4 In the tree, select the data class on which you want to view inventory data.
- 5 In the right pane, select the tab that contains the information you want to view.
- 6 (Optional) To export the data into a spreadsheet or HTML file, click **Save As**, click the file type, then select the data range, and click **OK**.

Depending on your needs, you can export all data, selected data, or filtered data.

Viewing event data for a data class

Using Resource Manager, you can view event data for a particular data class. The event data that is displayed depends on the data class selected. In general, you can view status and current data about the data class events.

To view event data for a data class

- 1 In the Symantec Management Console, on the **Manage** menu, click **Resource**.
- 2 In the **Select Resource** dialog box, select the resource you want to manage, and then click **OK**.
- 3 In **Resource Manager**, on the **View** menu, click **Events**.
See [“Accessing Resource Manager”](#) on page 363.
- 4 In the tree, select the data class on which you want to view event data.
- 5 In the right pane, select the tab that contains the information you want to view.
- 6 (Optional) To export the data into a spreadsheet or HTML file, click **Save As**, click the file type, then select the data range, and click **OK**.

Depending on your needs, you can export all data, selected data, or filtered data.

Adding a resource to an organizational group

The Add to organizational group dialog box lets you add the selected resource to an organizational group. A resource may appear once only in each organizational view.

To add a resource to an organizational group

- 1 In the Symantec Management Console, on the **Manage** menu, click **Resource**.
- 2 In the **Select Resource** dialog box, select the resource you want to manage, and then click **OK**.
- 3 In the left pane of **Resource Manager**, click the **Add to organizational group link**.
- 4 In the **Add to organizational group** dialog box, select the organizational group to which you want to add the resource.
- 5 Click **Ok**.

See [“Resource Manager tasks”](#) on page 365.

Resource Manager tasks

Resource Manager lets you perform several tasks on a resource. These tasks are available through the Resource Manager **Tasks** menu. The available tasks depend on the type of resource that is selected.

See [“About resource management”](#) on page 362.

Table 29-1 Resource Manager tasks

Task	Description
Access the task management portal	If the task you want to perform is not listed in the left pane, you can access the task management portal to find additional tasks.
Add a resource to an organizational group	You can add the selected resource to an organizational group or move it to a new organizational group. If you select an organizational group within an organizational view to which the resource is not already a member, the resource is added to the organizational group. If you choose an organizational group within an organizational view to which the resource is already a member, the newly selected organizational group replaces the previous organizational group.
Delete a resource	You can delete the selected resource from the Configuration Management Database (CMDB).
Merge duplicate company resources	(Company resources only) If there are two entries for the same company, you can use this feature to merge the entries together.

Table 29-1 Resource Manager tasks (*continued*)

Task	Description
Ping computers	You can use the Task menu Ping Computer option to ping the selected computer.
Schedule task	You can use the Task menu Schedule Task option to schedule the running of a job or task.
View an organizational summary	You can view (Summaries > Organizational Summary) the organizational groups to which the selected resource is a part.
View Calendar	<p>You can use the View menu Calendar option to view Notification Server schedule information in.</p> <p>See “Viewing the Notification Server internal schedule calendar” on page 95.</p>
View events	<p>You can view event data for a data class, including general information about the data class and the status of the data class.</p> <p>See “Viewing event data for a data class” on page 364.</p>
View inventory	<p>You can view inventory data for a data class, including general information about the data class and the status of the data class.</p> <p>See “Viewing inventory data for a data class ” on page 364.</p>
View resource associations	You can view the resources with which the selected resource is associated in the left pane. If you select the associated resource in the left pane, Resource Manager lets you manage that resource.
View resource details	When Resource Manager opens, the right pane provides details about the selected resource.
View the resource associations	<p>You can use the View menu Resource Association option to view resource association information. The resource association page displays information about the resource association type and the resource type names that are associated with the selected resource.</p> <p>See “Viewing and managing resource data with Notification Server reports” on page 368.</p>

Using Notification Server reports

This chapter includes the following topics:

- [About Notification Server reports](#)
- [Viewing and managing resource data with Notification Server reports](#)

About Notification Server reports

You can view and manage your resource data through Notification Server reports. These reports give you information about your managed and unmanaged computers and your Notification Server configuration. Installed solutions also provide the reports that give you information specific to that solution. For example, you can use these reports to learn about which events and automation policies Notification Server executes and how long they take.

Reports can be secured so that only appropriate users can run a report. In addition, reports are scoped so that they return only the data that the user who runs the report has permission to view. For example, if a manager runs a salary report, they obtain only the salaries of their managed employees.

Reports let you view information in various ways. You can see your information in tables or graphically in charts. You can also drill down on specific items in a report to obtain additional information.

See [“Viewing and managing resource data with Notification Server reports”](#) on page 368.

A wide range of reports are provided with Notification Server. You cannot modify these default reports, but you can clone them and edit the clone to meet your requirements. You can also create new custom reports.

Viewing and managing resource data with Notification Server reports

You can use reports to view and manage resource data. Reports retrieve data from the CMDB. See [“About Notification Server reports”](#) on page 367.

Table 30-1 Process for viewing and managing resource data with Notification Server reports

Step	Action	Description
Step 1	Extract the report results.	You need to select the report to use, and optionally set the user parameters and select the snapshot to use. See “Extracting Notification Server report results” on page 369.
Step 2	View the report results.	You can configure the report view to suit your requirements as follows: <ul style="list-style-type: none"> ■ Select the grid view or chart view to use, if any extra views have been set up for the report. ■ Group and order the columns in the grid view. ■ Display the results in a chart view, if chart views have been set up for the report. See “Viewing Notification Server report results” on page 370.
Step 3	(Optional) Use the report results.	You can use report results in any of the following ways: <ul style="list-style-type: none"> ■ Drill down into selected items for more detailed information. Drilling down into an item opens the appropriate view, which may be another report or the Resource Manager Console. ■ Perform actions on selected items. ■ Print the report results. See “Using Notification Server report results” on page 371.

Table 30-1 Process for viewing and managing resource data with Notification Server reports
(continued)

Step	Action	Description
Step 4	(Optional) Save the report results.	<p>You can save the report results in the following formats:</p> <ul style="list-style-type: none"> ■ File Spreadsheet (.csv) file, HTML file, and XML file types are supplied with Notification Server. Installed solutions may provide options for additional file types. See “Saving Notification Server report results as a file” on page 373. ■ Static filter See “Creating a static filter from Notification Server report results” on page 373. ■ Snapshot See “Saving Notification Server report results as a snapshot” on page 374. ■ Web part See “Saving Notification Server report results as a Web part” on page 375.

Extracting Notification Server report results

A set of reports is supplied with Notification Server, and installed solutions may add further reports.

Some reports have the user parameters that you can set when you extract the report results. User parameters are variables in the report query, and they make reports more flexible and powerful. For example, the Computer list by System Type and OS Name report has user parameters defined for both the system type and OS name. When you extract report results, you can specify the system type and OS name combination that you want to use by setting the appropriate parameters. Without user parameters, each report would have fixed values defined within the query. You would need to have a different report for each system type and OS name combination. Alternatively, you would need to modify the report query each time you wanted to extract results.

To minimize the load on Notification Server, large or frequently-used reports can be saved as snapshots. Creating snapshots lets all other users view the report results in the latest snapshot instead of each user running the report over again. The scheduled reports are normally run with the Administrator scope to ensure that all available data is included. When you view the report result set, the snapshot data is scoped accordingly. When you view report results, you can choose a snapshot to use. If you don't choose a snapshot, the results are extracted by running the report query in the CMDB.

This task is a step in the process for viewing and managing resource data with Notification Server reports.

See [“Viewing and managing resource data with Notification Server reports”](#) on page 368.

To extract Notification Server report results

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, select the report that you want to use.
- 3 (Optional) In the right pane, under **Parameters**, set the appropriate user parameters.

After you change any parameter, the parameters string becomes highlighted with yellow, to indicate that the parameters string and report results differ from the selection in parameters control. When you click **Run**, the parameters string and the report results get updated and the yellow highlight disappears.

See [“Defining parameters and value providers for a custom report”](#) on page 383.

- 4 If you want the report query to run automatically after opening the report page, check **Auto-run**. If **Auto-run** is not checked, the report query does not run automatically and you must click **Run** to get the report data.

Note, that by default the **SuppressReportAutoRun** is disabled and therefore you can disable and enable the **Auto-run** functionality. If you enable the **SuppressReportAutoRun**, the **Auto-run** check-box becomes inactive. In this case, after you open any report, the report query does not run automatically and you must click **Run** to get the report data.

You can enable or disable the **SuppressReportAutorun** functionality in **NS Configurator**, under **Core Settings > User Interface > Report > SuppressReportAutorun**.

See [“Configuring Notification Server settings with NS Configurator”](#) on page 55.

- 5 If you want to use a snapshot, in the **View** drop-down list, select the appropriate snapshot.

The options are predefined as follows:

- Current
- Latest Snapshot

Any additional snapshots that you have created are listed. Each is labeled with its creation date and time.

Viewing Notification Server report results

You can display the report results using the following views, if they have been configured for the report:

Grid view	Grid views are tables, with each result item displayed on a separate row. The available columns are defined in the report. You can change the column order and group the results according to the values in a particular column. For example, you may want to group a list of computers by operating system type or subnet.
Chart view	Chart views are graphical formats such as bar charts, line charts, pie charts, and area charts. Multiple chart views may be defined in the report, but you can view only one at a time.

Each chart or grid is a particular view into the report results, so a view may contain a subset of the results. A report may have multiple views that are available to customize the output for different users instead of different reports being created for each user. For example, a report that lists managed computers may include properties of each computer, such as operating system, processor type, and disk size. The report may have a number of different views, with each view containing a subset of the available properties for each computer. When you look at the report, you can choose the view that contains the properties that interest you.

When you save a report, you save all of the results that are in your scope. You are not restricted to the data that is displayed in the current view. When you print a report, you print the current view.

This task is a step in the process for viewing and managing resource data with Notification Server reports.

See [“Viewing and managing resource data with Notification Server reports”](#) on page 368.

To view Notification Server report results

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, select the report that you want to use.
- 3 In the right pane, in the **View** drop-down list, select the appropriate view.
Any grid views and chart views that have been created are listed.
- 4 (Optional) If you want to group the results, in the **Group By** drop-down list, select the appropriate column.
- 5 (Optional) If you want to change the column order, click in a column header and drag the column to the appropriate position.

Using Notification Server report results

You can drill down into the report results to obtain additional information. Drilling down into an item opens the appropriate view, which may be another report or the Resource Manager.

You can perform actions on resources directly from the report results. For example, you can run a report that lists all computers that meet specific criteria. You can then perform an action

on some or all computers. The available actions are those that apply to the selected resource type and that you have permission to perform.

You can print selected rows of results or all the report results.

This task is a step in the process for viewing and managing resource data with Notification Server reports.

See [“Viewing and managing resource data with Notification Server reports”](#) on page 368.

To drill down into report results

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, select the report that you want to use.
- 3 In the right pane, in the **View** drop-down list, select the appropriate view.
- 4 In the report results, click on the item for which you want additional information.

Note that the drill-down action may vary: it might be a single click, or it might be a double-click.

To perform actions on resources listed in report results

- 1 In the report results, select the resources on which you want to perform an action.
- 2 Click **Actions**, and then select the appropriate option.

Note that this function is not always available.

To print report results

- 1 If necessary, in the report results, select the rows of report results that you want to print.
- 2 Click **Print**.
- 3 In the **Print** dialog box, specify the following settings:

Parameters If you want to include the user parameter settings in the printed results, check **Include Parameters**.

Data range Choose one of the following options:

- Print All - Includes all report results.
- Print Selected Rows - Includes only the selected rows of report results.

- 4 Click **Print**.

A preview of the report printout is shown in a new browser window, and Windows Print dialog appears. The preview is the same as what you see when you save the report as HTML.

- 5 In the **Windows Print** dialog, select the appropriate options, and then click **Print**.

Saving Notification Server report results as a file

You can save the report results as a file. You can save all of the results, or you can select the results that you want to include. Options for Spreadsheet (.csv) file, HTML file, and XML file types are supplied with Notification Server. Installed solutions may provide options for additional file types.

This task is a step in the process for viewing and managing resource data with Notification Server reports.

See [“Viewing and managing resource data with Notification Server reports”](#) on page 368.

To save Notification Server report results as a file

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, select the report that you want to use.
- 3 (Optional) In the right pane, select the rows of report results that you want to include in the file.
- 4 Click **Save As**, and then click the appropriate file type.
- 5 In the **Save As** dialog box, specify the following settings:

Parameters	If you want to include the user parameter settings in the file, check Include Parameters .
Data range	Choose one of the following options: <ul style="list-style-type: none">■ Save All - Includes all report results in the filter■ Save Selected Rows - Includes only the selected rows of report results in the filter.

- 6 Click **Save**.
- 7 In the **Save Report** dialog box, select the folder in which to save the file, and then click **Save**.

Creating a static filter from Notification Server report results

You can create a new static filter by saving the results of a report. You can include all of the results, or you can select the results that you want to include.

See [“About resource filters”](#) on page 297.

This task is a step in the process for viewing and managing resource data with Notification Server reports.

See [“Viewing and managing resource data with Notification Server reports”](#) on page 368.

To create a static filter from Notification Server report results

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, select the report that you want to use.
- 3 (Optional) In the right pane, select the rows of report results that you want to include in the filter.
- 4 Click **Save As > Static Filter**.
- 5 In the **Save As Static Filter** dialog box, specify the appropriate settings:

Name	The default is the report name. If you want to change the name, type the appropriate filter name.
Choose a resource to base the filter on	This option applies to resource reports only. In the drop-down list, select the appropriate option.
Data range	Choose one of the following options: <ul style="list-style-type: none"> ■ Save All - Includes all report results in the filter. ■ Save Selected Rows - Includes only the selected rows of report results in the filter.

- 6 Click **Save**.

The new filter is stored in the Filters tree, in the Report Based Filters folder.

Saving Notification Server report results as a snapshot

You can save the current report results as a snapshot. For example, you may want to save a particular set of results and make them available to other users without re-extracting them from the CMDB. When you save a report as a snapshot, it is saved according to your scope. Only users who share the same security role can view the snapshot.

This task is a step in the process for viewing and managing resource data with Notification Server reports.

See [“Viewing and managing resource data with Notification Server reports”](#) on page 368.

To save Notification Server report results as a snapshot

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, select the report that you want to use.
- 3 In the right pane, click **Save As > Snapshot**.

The next time you open the report, the new snapshot will be available on the **View** drop-down list.

Saving Notification Server report results as a Web part

You can save a report as a Web part that you can use in a portal page. The Web part report is a copy of the report that is dynamic and fully functioning. The result set that is displayed in the portal page is refreshed when you open the page, so it is always up-to-date. The Web part report is independent of the original report, so any changes that you make to one are not propagated to the other.

See [“Creating and modifying Web parts”](#) on page 36.

This task is a step in the process for viewing and managing resource data with Notification Server reports.

See [“Viewing and managing resource data with Notification Server reports”](#) on page 368.

To save Notification Server report results as a Web part

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, select the report that you want to use.
- 3 In the right pane, click **Save As > Webpart**.
- 4 (Optional) In the **Save As Webpart** dialog box, edit the name the new Web part.
The default name should be suitable for most purposes.
- 5 (Optional) In the **Choose a webpart size** drop-down list, select the appropriate size.
The default is Small.
- 6 Click **Save**.
The new Web part is saved in the Settings\Console Settings\Webparts folder.

Creating custom Notification Server reports

This chapter includes the following topics:

- [Components of a custom Notification Server report](#)
- [Creating and modifying custom Notification Server reports](#)

Components of a custom Notification Server report

Notification Server reports are constructed from a standard set of components.

Table 31-1 The components of a custom Notification Server report

Component	Description
Data source	<p>The data source is the component that provides the report data. Custom reports and dynamic filters use the SQL queries that run on the CMDB to extract the appropriate data. Solutions may provide the reports that use other data sources, such as spreadsheets or CSV files.</p> <p>Custom reports and dynamic filters use an SQL query as the data source. You can define the query by writing the SQL from scratch, or by using the Query Builder.</p> <p>See “Defining a resource query for a custom report” on page 381.</p> <p>See “Defining an SQL query for a custom report” on page 382.</p>

Table 31-1 The components of a custom Notification Server report (*continued*)

Component	Description
Views	<p>A report view is a particular way that the report data is displayed. A view typically contains a subset of the report data. The data is presented in a way that is appropriate to a particular user role. You can choose the data columns to include in the view, and specify which is to be used as the primary axis.</p> <p>The available types of views are:</p> <ul style="list-style-type: none"> ■ Grid view View the report data in tabular format, with each item displayed on a separate row. ■ Chart view View the report data in graphical format, such as bar charts, line charts, pie charts, and area charts. ■ Templated text <p>Setting up a number of different views for a report lets you customize the report data for different users. You can use a single report for all users, rather than creating multiple reports to meet the requirements of different users.</p> <p>See “Creating or modifying a chart view for a custom report” on page 385.</p> <p>See “Creating or modifying a grid view for a custom report” on page 386.</p>
Parameters	<p>Parameters are variables in the report query that the user can set when they run the report.</p> <p>Using parameters can make reports more flexible and powerful. For example, the Computer list by System Type and OS Name report has the parameters that are defined for the system type and OS name. When you run this report, you can specify the system type and OS name combination that you want to use by setting the appropriate parameters. Without parameters, each report would have fixed values defined within the query.</p> <p>See “Defining parameters and value providers for a custom report” on page 383.</p>
Drilldowns	<p>A report drilldown is an action that is performed when the user clicks on an item in the report results. You can add drilldowns to a report to enable the user to obtain additional information through the report results.</p> <p>For each drilldown, you can specify the view on which the drilldown is available and how the user triggers the drilldown. You can also specify the action that is performed and the parameters to use in the action. You can set up multiple drilldowns for a report to perform different actions on different types of resources.</p> <p>See “Setting up drilldown actions for a custom report” on page 387.</p>

Creating and modifying custom Notification Server reports

Notification Server reports let you view and manage your resource data. These reports give you information about your managed and unmanaged computers, and your Notification Server configuration. A wide range of reports are provided with the Symantec Management Platform. You can also create your own custom reports to suit the needs of your organization. Notification Server reports retrieve data from the Configuration Management Database (CMDB).

The report data can be used in the following ways:

- The data source for an automation policy
- A Web part that displays current data on a portal page
- A resource report that lets the user drill down on a particular resource to view full details in the Resource Manager
- A trend report that shows data changes over time
- Multiple drilldown reports (for example, hierarchy reports) that let the user drill down on high-level data to view more detailed low-level data.

To create or modify a custom report, you need to define the components of the report in the **Custom Report Edit** page.

See [“Components of a custom Notification Server report”](#) on page 376.

Note: Some automation policies use a report as a data source, and may depend upon some particular results or parameters. When you modify a report, you need ensure that the changes do not affect any automation policies.

See [“Specifying the automation policy data source”](#) on page 334.

Table 31-2 Process for creating and modifying custom Notification Server reports

Step	Action	Description
Step 1	Create a new report, or select an existing report to modify.	Create a new report from scratch, or by cloning a default report that is supplied with Notification Server. You can modify any custom report that you have created, but cannot modify the default reports. See “Creating a custom Notification Server report” on page 380. See “Modifying an existing custom Notification Server report” on page 381.

Table 31-2 Process for creating and modifying custom Notification Server reports
(continued)

Step	Action	Description
Step 2	Create the report query.	<p>You can write the query SQL yourself or use the Query Builder to build the report query. The Query Builder is a user-friendly tool that lets you select the tables and fields that you want to use.</p> <p>See “Defining a resource query for a custom report” on page 381.</p> <p>You can also write the SQL code from scratch. Alternatively, you can copy the SQL from another filter or report and modify it to suit your requirements.</p> <p>See “Defining an SQL query for a custom report” on page 382.</p>
Step 3	Specify the value providers for parameters.	<p>If the report query includes parameters, you can define the corresponding value providers. The value provider lets the user set the appropriate value for the query parameter when they run the report.</p> <p>See “Defining parameters and value providers for a custom report” on page 383.</p>
Step 4	Create the report views.	<p>A report view typically contains a subset of the report results. The results are presented in a way that is appropriate to a particular user role. Setting up a number of different views for a report lets you customize the report results for different users.</p> <p>See “Creating or modifying a chart view for a custom report” on page 385.</p> <p>See “Creating or modifying a grid view for a custom report” on page 386.</p>
Step 5	Create the drill-downs.	<p>A report drilldown is an action that is performed when the user clicks on an item in the report results. You can configure drilldowns for a report to enable the user to obtain additional information through the report results.</p> <p>See “Setting up drilldown actions for a custom report” on page 387.</p>
Step 6	Specify the report properties.	<p>You can choose whether or not the report results are restricted to the scope of the user who runs the report. You can also choose to run the report only as a snapshot. To minimize the load on Notification Server, you may want to run large or frequently-used reports as snapshots.</p> <p>See “Specifying advanced properties of a custom report” on page 389.</p>
Step 7	Save the report.	<p>Save the changes to the new report or modified report.</p> <p>See “Creating a custom Notification Server report” on page 380.</p> <p>See “Modifying an existing custom Notification Server report” on page 381.</p>

Creating a custom Notification Server report

You can create your own custom reports and configure them to suit your requirements. You can create a new report from scratch, or by cloning a default report that is supplied with Notification Server.

This task is a step in the process for creating and modifying custom Notification Server reports.

See [“Creating and modifying custom Notification Server reports”](#) on page 378.

To create a custom Notification Server report

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, right-click the folder in which you want to add the new report, and then click **New > Report**.
- 3 Click one of the following:

Computer Report	The report query is a resource query, and the base template selects all computers. You can refine the query to select the computers that you want.
User Report	The report query is a resource query, and the base template selects all users. You can refine the query to select the users that you want.
Resource Report	The report query is a resource query, and the base template selects all resources (including all computers and all users). You can refine the query to select the resources that you want.
SQL Report	The report query is an SQL query. You can write your own SQL query to extract the data that you want from the CMDB. No template is applied and there are no restrictions on what you can write.

- 4 (Optional) In the right pane, specify the report name and description.
- 5 On the custom report edit page, specify the report components and report properties on the appropriate tabs.

For more information, click the page and then press **F1**.

- 6 To save the changes without leaving the edit mode, click **Apply**.
- 7 To preview the changes without leaving the edit mode, click **Preview**.
- 8 To save the changes and leave edit mode, click **Save Changes**.

Modifying an existing custom Notification Server report

You can modify your own custom reports at any time. You cannot modify any of the default reports that are supplied with Notification Server. If you want to modify a default report, you can clone the report to create a copy of it, and then edit the copy.

This task is a step in the process for creating and modifying custom Notification Server reports.

See [“Creating and modifying custom Notification Server reports”](#) on page 378.

To modify an existing custom Notification Server report

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, do one of the following:
 - Right-click the report that you want to modify, and then click **Edit**.
 - Click the report that you want to modify, and then in the right pane, in the upper right corner, click **Edit**.
- 3 (Optional) Modify the report name and description.
- 4 In the **Custom Report Edit** page, make your changes to the report components and report properties on the appropriate tabs.

For more information, click the page and then press **F1**.
- 5 To save the changes without leaving the edit mode, click **Apply**.
- 6 To preview the changes without leaving the edit mode, click **Preview**.
- 7 To save the changes and leave the edit mode, click **Save Changes**.

Defining a resource query for a custom report

When you create or modify your own custom Notification Server report, you can define a report query. For a computer report, user report, or resource report you need to define a resource query.

A resource query is based on the tables that are available in the Configuration Management Database (CMDB). The Query Builder is a user-friendly tool that provides a standard template and lets you select the tables and fields that you want to use. It helps you to define the query to suit your requirements. You do not need any SQL knowledge to define a resource query. The resource query is converted to SQL automatically, and the SQL is run on the CMDB to extract the appropriate resources.

When you have defined a resource query for your custom report, you can then convert a resource query to the equivalent SQL query. For example, you can use the Query Builder to define the structure of your query, convert it to SQL, and then modify the SQL directly. This process can be quicker and more efficient than writing the entire query in SQL from scratch.

When you create a new computer report, user report, or resource report, a resource query template is added to the report automatically. When you create a new filter, the same resource query template is added to the filter when you choose the Query Builder query mode. The base query in the template selects all computers, users, or resources, corresponding to the report type. You need to modify the base query to select the appropriate resources.

This task is a step in the process for creating and modifying custom Notification Server reports.

See [“Creating and modifying custom Notification Server reports”](#) on page 378.

To define a resource query for a custom report

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 Do one of following:
 - To define a resource query for a new report that you create, in the left pane, right-click the folder in which you want to add the new report. Then click **New** and click **Computer Report**, **User Report**, or **Resource Report**.
 - To redefine a resource query for an existing report, in the left pane, click the computer report, user report, or resource report that you want to modify. Then in the right pane, in the upper right corner, click **Edit**.
- 3 In the right pane, on the **Data Source** tab, specify the query details.
 For more information, click the page and then press **F1**.
- 4 (Optional) To convert the resource query to the equivalent SQL query, click **Convert this query to SQL Query**.

Warning: Converting a resource query to an SQL query is a one-way operation. You cannot convert the resulting SQL query back to a resource query.

- 5 Click **Save Changes**.

Defining an SQL query for a custom report

When you create or modify your own custom Notification Server report, you can define a report query. For a computer report, user report, or resource report you need to define a resource query for the report. For an SQL report, you need to define an SQL query.

You can write an SQL query to define the resources that you want to include in the report or filter. You can write the SQL code from scratch. Alternatively, you can copy the SQL from another filter or report and modify it to suit your requirements. For example, you can create a resource query using the Query Builder, and then copy the generated SQL from the Resolved Query tab. You can also use the Query Builder to define the structure of your query, convert it to SQL, and then modify the SQL directly.

When you create a new SQL report, an SQL query template is added to the report automatically. When you create a new filter, the same SQL query template is added to the filter when you choose the Raw SQL query mode. The base SQL query selects all available resources. You need to modify the base query to select the appropriate resources.

You need the Edit SQL privilege to create or modify SQL queries, and you should have a good understanding of the CMDB table structure. If you want any scoping that is applied to the query results, you need to include the appropriate SQL code in the query.

This task is a step in the process for creating and modifying custom Notification Server reports.

See [“Creating and modifying custom Notification Server reports”](#) on page 378.

To define an SQL query for a custom report

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 Do one of following:
 - To define an SQL query for a new report that you create, in the left pane, right-click the folder in which you want to add the new report. Then click **New** and click **SQL Report**.
 - To redefine an SQL query for an existing report, in the left pane, click the SQL report, that you want to modify. Then in the right pane, in the upper right corner, click **Edit**.
- 3 In the right pane, on the **Data Source** tab, specify the query details in the appropriate tabs.

For more information, click the page and then press **F1**.

- 4 Click **Save Changes**.

Defining parameters and value providers for a custom report

If the query of the custom report that you create or modify includes parameters, you can define the appropriate value providers. The value provider of a parameter lets the user set the appropriate value for the parameter when they run the report. Including user-definable parameters in a report query lets you create a single flexible report that can extract different result sets by changing the parameter values. The alternative would be to hard code the parameter values in the query. You would then need to modify the query each time you wanted to use a different parameter value. You can also create multiple reports with a different value defined in each query.

The value provider specifies how the parameter value is set when the user runs the report. In many cases the value provider is a UI component that accepts a value or setting from the user. For example, you can define the value provider of a parameter as a drop-down list with a set of valid values that the user can choose from. Alternatively, you can define the value provider as a text field that accepts a string of characters that the user types. In some cases, a parameter

does not require a value provider. The parameter value is set automatically with no user action required.

This task is a step in the process for creating and modifying custom Notification Server reports.

See [“Creating and modifying custom Notification Server reports”](#) on page 378.

To add a parameter to a custom report

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, select the report that you want to modify.
- 3 On the *Report Name* page, in the upper right corner, click **Edit**.
- 4 On the **Report Parameters** tab, do the following:

- | | |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To add a parameter | <p>Click Add, and then click the appropriate query parameter.</p> <p>The drop-down list contains all of the parameters that have been defined in the report query but have not yet been added to the report.</p> |
| To add an advanced type parameter | <p>Click Add > Advanced Types and then click the type that you want.</p> |
| To create a new parameter | <ul style="list-style-type: none"> ■ Click Add > New Parameter. ■ In the Editing Parameter dialog box, under Parameter, specify the appropriate parameter settings. ■ Under Value Provider, in the Name drop-down list, select the type of value provider that you want to use. ■ Under Configuration, specify the appropriate value provider settings. ■ Click OK. |

To modify a parameter

- Click the parameter that you want to modify, and then click the **Edit** symbol.
- In the **Editing Parameter** dialog box, under **Parameter**, specify the appropriate parameter settings.
- Under **Value Provider**, in the **Name** drop-down list, select the type of value provider that you want to use.
The options that are available depend on the parameter type setting that you made under **Parameter**.
- Under **Configuration**, specify the appropriate value provider settings.
If you want to view or edit another parameter in the list, click the up and down buttons to display the details of the appropriate parameter.
- Click **OK**.

5 Click **Save Changes**.

Creating or modifying a chart view for a custom report

When you create or modify your own custom Notification Server report, you can define a report view. A report view is a particular way that the report results are displayed. Setting up a number of different views for a report lets you customize the report results for different users. A chart view lets you view the report results in graphical format, such as bar charts, line charts, pie charts, and area charts.

Note: A third-party tool set provides the functionality that is used in chart views. For full descriptions of charting components, refer to the documentation that [Dundas Data Visualization, Inc. \(Dundas.com\)](http://Dundas.com) provides.

This task is a step in the process for creating and modifying custom Notification Server reports. See “[Creating and modifying custom Notification Server reports](#)” on page 378.

To create or modify a chart view for a custom report

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, select the report that you want to modify.
- 3 On the *Report Name* page, click **Edit**.
- 4 On the **Views** tab, do one of the following:
 - To create a new chart view, click **Add**.
 - To modify an existing chart view, in the **View** drop-down list, select the view that you want to modify.

- 5 (Optional) In the **Name** box, type the chart view name.
- 6 In the **Type** drop-down list, click **Chart**.
- 7 In the **Chart Type** drop-down list, click the type of chart that you want to use.
- 8 In the **Chart Style** drop-down list, click the style that you want to use for rendering the chart.

A chart style is a predefined set of the colors that can be used for rendering the chart.

- 9 In the **Size** boxes, specify the height and width of the chart in pixels.
- 10 In the **Chart Labels** drop-down list, select the appropriate option:

All	Shows both the actual data values and the percentages.
Values	Shows the actual data values, such as the number of items of each type.
Percentage	Shows the data as percentages, such as the percentage of items of each type.
None	No labels are shown.
X Axis Only	Shows the data values for the X axis only. The Y axis is not labeled.

- 11 Set up the chart view by specifying the appropriate settings on the following tabs:

Title	Lets you specify the chart title text, and the location at which it appears.
Legend	Lets you specify the chart legend text, and the location at which it appears.
3D	Lets you set up 3D zooming. 3D zooming lets you enlarge selected areas of the chart to the full window size.
X Axis	Lets you choose the result column to use as the X axis in the chart, specify the title text, and configure the appearance of the X axis.
Y Axis	Lets you choose the result columns to use as the Y axis in the chart, specify the title text, and configure the appearance of the Y axis.

For more information, click the page and then press **F1**.

- 12 Click **Save Changes**.

Creating or modifying a grid view for a custom report

When you create or modify your own custom Notification Server report, you can create and modify the grid views that you want in your reports. For each grid view, you can select the result columns to include and specify how the results are formatted.

This task is a step in the process for creating and modifying custom Notification Server reports.

See [“Creating and modifying custom Notification Server reports”](#) on page 378.

To create or modify a grid view for a custom report

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, select the report that you want to modify.
- 3 On the *Report Name* page, in the upper right corner, click **Edit**.
- 4 On the **Views** tab, do one of the following:

To create a new grid view Click **Add**.

To modify an existing grid view In the **View** drop-down list, select the view that you want to modify.

- 5 (Optional) In the **Name** box, type the view name.
- 6 In the **Type** drop-down list, select **Grid**.
- 7 On the **Hidden Columns** tab, specify the data columns to include in the grid view of the custom report.

By default, the grid view includes all columns in the query results. You can hide any data columns that you do not want to display to the user.

- 8 On the **Advanced Formatting** tab, set up a formatting template that applies HTML tagging to appropriate cells or rows in the report results.

For example, in a computer disk space report you might want to highlight all the computers that have less than a specified minimum free space remaining. You can create a template that formats the relevant rows with a bright yellow background and uses bold text in the free space cell.

For more information, click the page and then press **F1**.

- 9 (Optional) To preview the grid using the current settings, click **Preview**.
- 10 Click **Save Changes**.

Setting up drilldown actions for a custom report

When you create or modify your own custom Notification Server report, you can set up a report drilldown. A report drilldown is an action that is performed when the user clicks on an item in the report results. You may want to configure drilldowns for a report to enable the user to obtain additional information through the report results. Drilling down into an item opens the appropriate view, which may be another report or a URL (such as the Resource Manager Console).

You can set up multiple drilldowns for a report to perform different actions on different types of resources.

For each drilldown, you can specify the view on which the drilldown is available, and how the user triggers the drilldown. You can also specify the action that is performed and the parameters that are used in the action.

You can create multiple drill-down reports, which are groups of the reports that are linked in a hierarchical structure. This structure can enable the report user to select an item in a report result-set and run further reports on it. Drill-down reports can present expanded information for a smaller set of resources, or can provide different information on the resource by reporting on different fields.

This task is a step in the process for creating and modifying custom Notification Server reports.

See [“Creating and modifying custom Notification Server reports”](#) on page 378.

To set up drilldown actions for a custom report

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, select the report that you want to modify.
- 3 On the *Report Name* page, click **Edit**.
- 4 On the **Drilldowns** tab, do one of the following:

To add a new drilldown	Click Add .
------------------------	--------------------

To modify an existing drilldown	In the Drilldown drop-down list, select the drilldown that you want to modify.
---------------------------------	---------------------------------------------------------------------------------------

- 5 In the **Name** box, type an appropriate name for the drilldown.
- 6 Under **Action Wireup**, specify the following settings:

Available On	Lets you specify the appropriate report view.
---------------------	-----------------------------------------------

Event	Lets you specify the user event that is required to perform the drilldown.
--------------	----------------------------------------------------------------------------

Performs	Lets you specify the action that the drilldown performs. Depending on the action that you select, the options under Action Configuration change.
-----------------	------------------------------------------------------------------------------------------------------------------------------------------------------------

7 Under Action Configuration, specify the following:

Drilldown To Report	In the Report Item drop-down list, select the report that you want the drilldown action to run.
Show Context Menu	Not applicable.
Open a URL in a new Window	In the Open URL box, type the URL of the item that you want the drilldown action to open, and then click Set .
Open a URL in a new Window for the Remote NS	In the Remote Report Item GUID box, type the GUID of the remote report that you want the drilldown action to open, and then click Set .

8 Under Passing Parameters, set up the parameters that pass values to the drilldown action.

Add or edit the following options of the parameter:

Source	The source of the parameter value: <ul style="list-style-type: none"> ■ Named Parameter ■ First Selected Value ■ Selected Row ■ Entire Selection
Field Info	The name of the source field.
Target Parameter	The parameter name.
Target Parameter Type	The parameter type. The drop-down list contains all of the available parameter types.

You need to match properties or values from the selected item to the parameters in the drilldown action. This process ensures that the appropriate action is performed. For example, if you want the drilldown action to open the Resource Manager, you can pass the appropriate resource GUID as a parameter. If you want the drilldown action to run a report, you can pass the appropriate values for the report query.

9 Click Save Changes.

Specifying advanced properties of a custom report

When you create or modify your own custom Notification Server report, you can restrict the report results to the scope of the user who runs the report. By default, running a report extracts the full (unscoped) set of results from the CMDB. The report results may then be scoped to

ensure that the user sees only the appropriate data. However, you can apply scoping to the report so that only the appropriate data is extracted from the CMDB.

You can also choose to run the report only as a snapshot. To minimize the load on Notification Server, you may want to run large or frequently-used reports as snapshots. When a user runs the report, the results are obtained from the latest snapshot, rather than by running the report query on the CMDB. When you set a report to run only as a snapshot, you can optionally specify the maximum age of the snapshot. When the snapshot reaches this age, the report query is run on the CMDB to extract the latest result set and update the snapshot.

This task is a step in the process for creating and modifying custom Notification Server reports.

See [“Creating and modifying custom Notification Server reports”](#) on page 378.

To specify advanced properties of a custom report

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, select the report that you want to modify.
- 3 On the *Report Name* page, click **Edit**.
- 4 On the **Advanced** tab, do any of the following:

To promote scoping information to the data source Check **Promote scoping information to the data source**.

- To run the report only as a snapshot
- 1 Check **Always run report as a snapshot**.
 - 2 In the **Automatically refresh snapshot when older than** box, specify the age at which to update the snapshot with the latest report results.

- 5 Click **Save Changes**.

Viewing resource information

This chapter includes the following topics:

- [About resources](#)
- [Viewing resource data class information](#)
- [Viewing resource association type information](#)
- [Viewing resource type information](#)

About resources

Resources are the items with which Notification Server works and stores data about, such as assets, invoices, purchase orders, projects, contracts, and users. Data about a resource is added to the Configuration Management Database (CMDB) using a template that is called a resource type. Each resource in the CMDB has a resource type that specifies the information that is recorded about the resource. For example, the resource name, description, model, asset tag number, owner, department, and so on.

The more resources you work with, the more you need to group resources together for management purposes. You can use organizational views, organizational groups, and resource filters to help group your resources.

See [“Viewing resource data class information”](#) on page 392.

See [“Viewing resource association type information”](#) on page 392.

See [“Viewing resource type information”](#) on page 392.

Viewing resource data class information

You can view resource data class information. A resource data class defines one or more fields, and the properties of the fields, that a resource of that class may have.

See [“About resources”](#) on page 391.

To view resource data class information

- 1 In the Symantec Management Console, in the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand the **Settings > Notification Server > Resource and Data Class Settings > Data Classes** folder, and then select the appropriate data class.

Viewing resource association type information

You can view resource association type information. A resource association is a link between two resources, such as between a user and a computer. The user of a computer has an association with that computer, and vice versa.

See [“About resources”](#) on page 391.

To view resource association type information

- 1 In the Symantec Management Console, in the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand the **Settings > Notification Server > Resource and Data Class Settings > Resource Associations** folder, and then select the appropriate resource association type.

Viewing resource type information

You can view resource type information, such as the base resource type and resource associations that apply to the resource type. You can also view the data classes that are included in the resource type.

See [“About resources”](#) on page 391.

To view resource type information

- 1 In the Symantec Management Console, in the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand the **Settings > Notification Server > Resource and Data Class Settings > Resource Types** folder, and then select the appropriate resource type.
- 3 On the **Resource Type Information** page, on the **Configuration** tab, view the following resource type information:

Resource type details

Resource type name, description, and the base resource type.

Association Types

Resource Associations that apply to the resource type. By default, only those that are applied directly are displayed.

To show all resource associations, check **Show inherited association types**.

Data Classes

The data classes that are included in the resource type. By default, all data classes are displayed.

To change the view:

- 1 Click one of the following:

Editable - show the data classes that you can edit.

All - show all data classes.

This selection operates on the available data classes.

- 2 (Optional) To hide inherited data classes, uncheck **Show inherited data classes**.

Any changes that you make are not preserved when you leave the **Resource Type Information** page. The default settings are restored the next time that you open the page.

About Symantec Remote Access Connector

This chapter includes the following topics:

- [Setting up Symantec Remote Access Connector](#)
- [Symantec Remote Access Connector configuration file](#)
- [Creating the Remote Access Connector configuration file template](#)
- [Importing the Remote Access Connector configuration file](#)
- [Using a remote connection tool from Symantec Management Console](#)

Setting up Symantec Remote Access Connector

Symantec Remote Access Connector is an IT Management Suite application that lets you configure and integrate the following third-party remote connection tools with IT Management Suite:

- Microsoft Remote Desktop Connection
- Bomgar Remote Support Solution
- XVUE Remote Desktop Client
- SimpleHelp Remote Support
- Splashtop Business for Remote Support

You can then use the third-party tool to connect to a client computer.

Note: Symantec Remote Access Connector is available when you install Client Management Suite or IT Management Suite. You can also install Symantec Remote Access Connector individually along with Symantec Management Platform.

The Remote Access Connector tool has the following highlights:

- You do not require a license to use the Remote Access Connector tool. However, you do require a license for the third-party remote connection tool that you want to integrate with IT Management Suite.
- You can integrate more than one remote connection tool. The multiple tools can be accessed from the right-click option in Symantec Management Console.
 See [“Using a remote connection tool from Symantec Management Console”](#) on page 400.
- You can install Remote Access Connector individually or as a part of Client Management Suite.

To use the Remote Access Connector, you must create or configure the Remote Access Connector configuration file and then import it to enable the right-click menu options in the Symantec Management Console.

Table 33-1 Setting up Remote Access Connector

Step	Action	Description
Step 1	Create the configuration file.	Create a configuration file based on the suggested template. You can also modify the default file according to your requirements. See “Symantec Remote Access Connector configuration file” on page 395. See “Creating the Remote Access Connector configuration file template” on page 399.
Step 2	Import configuration file.	Importing the configuration file enables the right-click menu options in the Symantec Management Console. See “Importing the Remote Access Connector configuration file” on page 399. See “Using a remote connection tool from Symantec Management Console” on page 400.

Symantec Remote Access Connector configuration file

The Symantec Remote Access Connector configuration file lets you add or modify the configuration details to enable the use of a third-party remote connection tool.

You can edit the configuration file, an XML-based file, to add information to connect with the following third-party remote tools:

- Microsoft Remote Desktop Connection
- Bomgar Remote Support Solution
- XVUE Remote Desktop Client
- SimpleHelp Remote Support
- Splashtop Business for Remote Support

The content of the default configuration file is the following:

```
xml version="1.0" encoding="utf-8" ?>
<remoteTools>
  <remoteTool Name="MS RDP">
    <API type="EXE">
      <exeFullPath>%windir%\system32\mstsc.exe</exeFullPath>
      <parameters>-v [HOSTNAME]</parameters>
    </API>
  </remoteTool>

  <!--
  <remoteTool Name="Bomgar Remote">
  <API type="HTTP">
  <URL>https://support.example.com/api/client_script?type=rep&operation=generate&
  </API>
  </remoteTool>
  <remoteTool Name="Bomgar Connect">
  <API type="HTTP">
  <URL>https://support.example.com/api/client_script?type=rep&operation=generate&
  </API>
  </remoteTool>
  <remoteTool Name="SimpleHelp">
  <API type="HTTP">
  <URL>simplehelp://?JW_machine_filter=</URL>
  </API>
  </remoteTool>
  <remoteTool Name="XVUE">
  <API type="HTTP">
  <URL>xvue://?JW_machine_filter=</URL>
  </API>
  </remoteTool>
  <remoteTool Name="Splashtop">
  <API type="HTTP">
```

```
<URL>st-business://com.splashtop.business/?account=username@company.com&autologin=
</API>
</remoteTool>
-->
</remoteTools>
```

Note: By default, Microsoft RDP tool is enabled and rest tools are commented. To use any tool, user can remove the comment of the required tool node and provide the details.

1. For Bomgar tool, replace the valid Bomgar instance URL with support.example.com value in <URL> node.
2. For Splashtop, replace the valid SplashTop user account details with username@company.com value in <URL> node.

Table 33-2 Tags used in the configuration file

Attributes	Description
remoteTool Name	<p>You can provide a short name of the remote tool. The short name is seen in the right-click menu option when you try to access the remote tool from the Symantec Management Console.</p> <p>Warning: If this attribute is not present or the value is empty, the system will not import the configuration file and display an error.</p>
API type	<p>This tag describes the type of API connection. The values can be HTTP or EXE. For the HTTP type, you must provide the API URL for the third-party tool. If you update the third-party tool, you must verify the URL.</p> <p>For Bomgar API URL, refer to the Bomgar API Programmer's Guide at the following location:</p> <p>https://www.bomgar.com/docs/content/integrations/api/index.htm</p> <p>For the EXE type, you must provide the full path of the remote tool that is available on the Notification Server computer. You can also add the path as an environment variable for ease of use. If you access Symantec Management Console from a different computer, ensure that the remote tool is installed on the computer.</p> <p>The default file contains configuration for Microsoft® Remote Desktop Connection application.</p> <p>Warning: If this attribute is not present or the value is empty, the system will not import the configuration file and display an error.</p>

To include the details of a third-party tool in the configuration file, add the required syntax before the </remoteTools> XML tag.

Table 33-3 Syntax for supported third-party remote connection tools

Remote Tool Name	Syntax
Microsoft Remote Desktop Connection Note: Present by default	<pre><remoteTool Name="MS RDP"> <API type="EXE"> <exeFullPath>%windir%\system32\mstsc.exe</exeFullPath> <parameters>-v [HOSTNAME]</parameters> </API> </remoteTool></pre>
Bomgar Remote Support Solution	<pre><remoteTool Name="Bomgar"> <API type="HTTP"> <URL>https://support.example.com/api/client_script?type=rep& operation=generate&action=start_pinned_client_session& search_string=</URL> </API> </remoteTool></pre>
XVUE Remote Desktop Client	<pre><remoteTool Name="XVUERDC"> <API type="HTTP"> <URL>xvue://?JW_machine_filter=</URL> </API> </remoteTool></pre>
SimpleHelp Remote Support	<pre><remoteTool Name="SimpleHelp"> <API type="HTTP"> <URL>simplehelp://?JW_machine_filter=</URL> </API> </remoteTool></pre>
Splashtop Business for Remote Support	<pre><remoteTool Name="Splashtop"> <API type="HTTP"> <URL>st-business://com.splashtop.business/? account=username@company.com&autologin=1&mac=</URL> </API> </remoteTool></pre>

See [“Creating the Remote Access Connector configuration file template”](#) on page 399.

Creating the Remote Access Connector configuration file template

The default Remote Access Connector configuration file is available after the installation of IT Management Suite at the following location:

```
<install directory>\Program Files\Altiris\Notification  
Server\NSCap\bin\Win32\X86\RemoteTemplate
```

See [“Symantec Remote Access Connector configuration file”](#) on page 395.

However, if required, you can recreate the default configuration file template and save it at another location.

The default file contains configuration for Microsoft Remote Desktop Connection application.

To create the Remote Access Connector configuration file template

- 1 In the Symantec Management Console, on the **Settings** menu, click **Console > Remote Tool Integration > Create Template Configuration**.
- 2 Save the `RemoteToolTemplate.config` file at an accessible location.

Importing the Remote Access Connector configuration file

You can customize the default configuration file template if required and import the modified file to access the third-party remote connection tool.

The following validation checks are performed while you import the configuration file:

- The `<remoteTools>` and `<remoteTool>` nodes are present.
- The `<remoteTool>` attribute `Name` is present and the value is not empty.
- The `<API>` node is present.
- The `<API>` attribute `<type>` is present and the value is either `HTTP` or `EXE`.
- If the `<API>` attribute `<type>` is `HTTP`, then the child node `<URL>` is present and the value is not empty.
- If the `<API>` attribute `<type>` is `EXE`, then the child node `<exeFullPath>` is present and the value is not empty.
- If the `<API>` attribute `<type>` is `EXE`, then the second child node is `<parameteres>`.

See [“Setting up Symantec Remote Access Connector”](#) on page 394.

See [“Symantec Remote Access Connector configuration file”](#) on page 395.

See [“Using a remote connection tool from Symantec Management Console”](#) on page 400.

To import the Remote Access Connector configuration file

- 1 In the Symantec Management Console, on the **Settings** menu, click **Console > Remote Tool Integration > Import Configuration**.
- 2 In the **Import configuration of remote tool** dialog box, click **Browse...**, select the `.config` file, and then click **Import**.

Warning: If the configuration file size exceeds 4 MB, then the application displays an error.

Using a remote connection tool from Symantec Management Console

To enable the right-click menu in the Symantec Management Console for remote access, you must import the configuration file.

See [“Importing the Remote Access Connector configuration file”](#) on page 399.

To use a remote connection tool from Symantec Management Console

- 1 In the Symantec Management Console, on the **Manage** menu, click **Computers**.
- 2 In the computers list, right-click a computer, click **Remote Access**, and then select the tool that you want to use. For example, select Microsoft Remote Desktop Connection or Bomgar Remote Support Solution.
- 3 For using Microsoft Remote Desktop Connection tool, save the file on Notification Server to start using it.

This `.bat` file contains the information that Notification Server requires to access the third-party remote tool.

For other third-party remote connection tools, you can directly start the application.

Configuring Symantec Security Cloud Connector

This chapter includes the following topics:

- [Setting up Symantec Security Cloud Connector](#)

Setting up Symantec Security Cloud Connector

Symantec Security Cloud Connector lets you integrate Symantec Endpoint Protection Cloud service with your IT Management Suite. You can manage the mobile devices of your organization in the Endpoint Protection Cloud portal, import the data into IT Management Suite, and then view the data in the Symantec Management Console.

Table 34-1 Process for setting up Symantec Security Cloud Connector

Step	Action	Description
Step 1	Create a Symantec Security Cloud account.	You create the Symantec Security Cloud account at the following URL: https://securitycloud.symantec.com For more information about getting started with Symantec Security Cloud , see the Endpoint Protection Cloud Help .
Step 2	Set up Endpoint Protection Cloud .	After you create the Symantec Security Cloud account, you can set up the security policies and settings for your users and their devices. For more information about working with Endpoint Protection Cloud , see the Endpoint Protection Cloud Help .

Table 34-1 Process for setting up Symantec Security Cloud Connector (*continued*)

Step	Action	Description
Step 3	Configure the Client Application access for Notification Server.	<p>To configure the Client Application access for Notification Server:</p> <ol style="list-style-type: none"> 1 In the Symantec Endpoint Protection Cloud portal, click Settings, and then go to Client Application Management. 2 On the Client Application Management page, click Add Client Application. 3 In the Add Application dialog box, make sure that, in the Application drop-down list, IT Management Suite (ITMS) is selected, and then click Add. <p>Note: To create a connector in ITMS, you need the Client ID and Client Secret values of the created Client Application.</p>
Step 4	Create a connector.	<p>To create a connector:</p> <ol style="list-style-type: none"> 1 In the Symantec Management Console, on the Settings menu, click Security Cloud Connector. 2 On the Connector Configuration page, click Create New Connector. 3 Follow the steps in the Configure Security Cloud Connector wizard. <p>One connector handles one Symantec Security Cloud account. To import data from several accounts, you must create a connector for each account.</p> <p>By default, only the users with Symantec Administrators role can create and manage the connectors.</p>

Table 34-1 Process for setting up Symantec Security Cloud Connector (*continued*)

Step	Action	Description
Step 5	View the imported Cloud data.	<p>During the synchronization, the following resource types are imported:</p> <ul style="list-style-type: none"> ■ Computers The imported computers that are also found in CMDB are merged with the existing resources. The imported computers that are not in CMDB become unmanaged devices. ■ Mobile Devices The imported mobile devices become unmanaged devices. ■ Groups and their hierarchical structure ■ Users Users are imported together with their relations to Computer or Mobile Device resources. Imported users are not merged with the users in CMDB. <p>During the first-time import and if the import interval is one day or more, the full data import is performed. The full data import is also performed after you edit the settings of the connector or click Synchronize Now. Delta update is performed when the import interval is less than one day and the last import task was successful.</p> <p>You can use the Symantec Security Cloud filters and filter criteria to view and search for the imported data.</p> <p>On the filter summary view flipbook, on the Security Status page, you can see the security status of all devices that are imported from the Endpoint Protection Cloud portal. Endpoint Protection Cloud inventory is displayed on the General page on the device details flipbook. Endpoint Protection Cloud user names are visible with the associated device names.</p>
Step 6	(Optional) Edit the settings of the connector.	<p>Depending on your requirements, you can change the settings of the data import from Endpoint Protection Cloud to IT Management Suite.</p> <p>To edit a connector:</p> <ol style="list-style-type: none"> 1 In the Symantec Management Console, on the Settings menu, click Security Cloud Connector. 2 On the Connector Configuration page, select the connector that you want to edit, and then click the Edit icon on the toolbar. 3 On the connector edit page, edit the necessary settings, and then click Save changes.

Managing CMDB data with Data Connector

- [Chapter 35. Introducing Data Connector](#)
- [Chapter 36. Performing data management tasks](#)

Introducing Data Connector

This chapter includes the following topics:

- [About Data Connector](#)
- [How Data Connector works](#)
- [What you can do with Data Connector](#)

About Data Connector

Data Connector is a component of the Symantec Management Platform that lets you transfer data between external data sources and the Configuration Management Database (CMDB). The ability to transfer data lets you leverage the data that already exists in the CMDB or other applications. Data transfers can be scheduled, so updates can be regularly, and automatically made to keep data current. Data Connector supports many data formats: OLEDB, ODBC, LDAP, XML, and CSV.

Data Connector also lets you manipulate the data that is already in the CMDB. This ability lets you easily normalize and correct errors in your data. For example, you can use Data Connector to normalize company names so data is consistent.

See [“How Data Connector works”](#) on page 405.

How Data Connector works

Data Connector transfers data by using data source definitions and data transfer rules. A data source definition defines the parameters for working with a particular data source or data recipient (referred to in general as data source). The parameters can include the data source location, name, type of data transfer, and the credentials that are required to access the data source.

Data Connector supports CSV, LDAP, ODBC, OLEDB, and XML data source types.

A data transfer rule configures the details of a data transfer, such as the following:

- A data source definition that is used for the transfer
- The resource type that is involved in the transfer
- Mappings between the fields that are involved in the transfer
- Whether the transfer is an import or an export

Different types of data transfer rules are available for different types of data transfer:

Bulk resource export	An efficient way of exporting bulk resources from a report or a resource target into a Notification Server Event (NSE) XML file. You can also use this rule type to export resource change histories.
Filter import	Specifies the Symantec Management Platform filter membership by importing the filter membership from a data source.
Organizational group import	Specifies the Symantec Management Platform organizational view and group memberships by importing the organizational view or group membership from a data source.
Report export	Exports report data to a data source that has a data source definition that allows exporting.
Resource data transfer	Transfers (imports or exports) the resource data between a data source and the CMDB.

To automate the process of transferring data, you can schedule each data transfer rule to run at a specific time. Data transfer rules can also be run through Symantec Management Platform tasks. After data transfers, you can use predefined reports and log files to help you analyze the results of data transfers.

Data Connector also lets you manipulate the data that is already in the CMDB through CMDB rules. These rules let you normalize data or fix other consistency problems with your CMDB data. To manipulate the CMDB, you need CMDB Solution.

See [“About Data Connector”](#) on page 405.

See [“What you can do with Data Connector”](#) on page 406.

What you can do with Data Connector

Data Connector lets you transfer data between the CMDB and a data source and manipulate data within the CMDB.

You can perform the following data transfer activities with Data Connector:

- Transfer (import and export) resource data between a data source and the CMDB.

See [“Importing and exporting data”](#) on page 408.

- Import filter membership information, including adding or removing the membership of resources from one or more filters.
- Import organizational view and group memberships.
- Export a report.
- Export resource data in bulk.

Data Connector also lets you manipulate data within the CMDB. For example, you can normalize or change a set of data within the CMDB. To manipulate the data within the CMDB, you must have CMDB Solution.

Performing data management tasks

This chapter includes the following topics:

- [Importing and exporting data](#)
- [Creating a virtual data class](#)
- [Configuring data connector verbose log purging options](#)

Importing and exporting data

You need to perform several steps to transfer the data between the Configuration Management Database (CMDB) and a data source.

Table 36-1 Process for importing and exporting data

Step	Action	Description
Step 1	Create a data file.	<p>First, you must create a data file and populate it with values. You can enter the data manually or through an external process. When you add column names as a first row in the data file, the data import rule lets you match up the columns to the CMDB data classes more easily.</p> <p>You can also pre-process the data in the external data source before you import it into the CMDB.</p> <p>See “About pre-processing data before data imports” on page 409.</p>

Table 36-1 Process for importing and exporting data (*continued*)

Step	Action	Description
Step 2	Create a data source.	<p>You define data sources using data source definitions. Data source definitions define the parameters that must be specified to work with the data source. For example, a data source definition can define database or file locations, server names, and access credentials.</p> <p>See “Creating a data source definition” on page 410.</p>
Step 3	Create a data transfer rule.	<p>Data transfer rule lets you configure the data transfer. Data transfer rules specify the parameters of the data transfer, such as the schedule for data transfer, the input and output data table mappings, and the direction of data transfer.</p> <p>See “Creating a data transfer rule” on page 411.</p>
Step 4	(Optional) Create a resource lookup key.	<p>A resource lookup key is a set of data class columns that is used to match-up the resources between the CMDB and the data source.</p> <p>See “Creating a resource lookup key” on page 411.</p>
Step 5	(Optional) Run data transfer rule as a task.	<p>You can schedule a task to run data transfer rule.</p> <p>See “Running a data transfer rule as a task” on page 412.</p>
Step 6	Check the results of a data transfer.	<p>You can use predefined reports to verify that data transfers occurred successfully.</p> <p>See “Viewing data transfer summaries” on page 413.</p>
Step 7	(Optional) Check the health of data transfer rules.	<p>You can check the health of data transfer rules. Health checking ensures that there are no problems caused by changes to the rule that may prevent a data transfer from completing successfully.</p> <p>See “Checking the health of data transfer rules” on page 413.</p>
Step 8	(Optional) Manage the imported data.	<p>You can create the CMDB rules that let you clean up, normalize, or make bulk changes to the data in the CMDB.</p> <p>See “Creating a CMDB rule to edit CMDB data” on page 414.</p> <p>See “Running a CMDB rule as a task” on page 414.</p>

About pre-processing data before data imports

When importing data from an external data source into the Configuration Management Database (CMDB), you can manipulate the data before the data is imported. This data pre-processing lets you manipulate the data in the data source without changing the data in its original source.

You write a data pre-processing function using C# programming. The amount of pre-processing that you can do is limited only by what you can do with C# programming. A data pre-processing function in C# takes a data table as an input parameter. You can write C# code to manipulate the data table and its content. An updated data table is then returned as the return value of the method. The returned data table is the data for the data source during import.

To better understand how pre-processing might be used, consider the following example. You have an OLEDB data source configured to use "Table A" from "Database A". A pre-processing function dynamically adds a new column to the table. It also populates the new column with data derived from the other columns in the table.

This task is an optional step in the process for importing and exporting data.

See ["Importing and exporting data"](#) on page 408.

Creating a data source definition

A data source is a source or recipient of Configuration Management Database (CMDB) data. For example, a CSV file or an ODBC database can be a data source.

You can transfer data between the following data source types and the CMDB:

- CSV
- LDAP
- ODBC
- OLEDB
- XML
- Custom

A data source definition specifies how to access a particular data source. The definition includes the data source type, location, table name, and authentication information. For each data source to or from which you want to transfer data, you need a data source definition. For different data source types, there are different data source definition types. Some data source definition types allow importing and exporting of data from the CMDB. Other types only allow exporting or importing.

You must create a data source definition for each data source between which you want to transfer data.

This task is a step in the process for importing and exporting data.

See ["Importing and exporting data"](#) on page 408.

To create a data source definition

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Settings > Notification Server > Connector**.

- 3 Right-click **Data Sources**, and then click **New > Data Source**.
- 4 In the right pane, specify the appropriate values.
For more information, click the page and then press **F1**.
- 5 (Optional) Click **Test data source** to test access to the data source.
- 6 Click **Save changes**.

Creating a data transfer rule

Before you can transfer data between the Configuration Management Database (CMDB) and a data source, you need to specify the options of the data transfer. For example, you must specify the following:

- What type of data is transferred
- Whether the data is imported from or exported to the data source
- Which of the data is transferred from the data source
- When data transfer occurs

To specify the options of a data transfer, you use a data transfer rule. Several types of data transfer rules are available. The one you use depends on the type of information that you want to transfer.

Before you use a data transfer rule in a production environment, Symantec recommends that you test the rule. Use the **Test rule** option on the applicable data transfer rule page.

This task is a step in the process for importing and exporting data.

See [“Importing and exporting data”](#) on page 408.

To create a data transfer rule

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Settings > Notification Server > Connector**.
- 3 Right-click **Import/Export Rules**, and then click **New > Data Transfer Rule**.
- 4 In the right pane, specify the column mappings and a schedule for the rule.
For more information, click the page and then press **F1**.
- 5 Click **Save changes**.

Creating a resource lookup key

A resource lookup key is a unique value for a resource type that is used to match-up the resources between the Configuration Management Database (CMDB) and the data source.

This task is a step in the process for importing and exporting data.

See [“Importing and exporting data”](#) on page 408.

To create a resource lookup key

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Settings > Notification Server > Connector**.
- 3 Right-click **Resource Lookup Keys** and then click **New > Resource Lookup Key**.
- 4 In the right pane, specify the following settings:

Target Resource Type	Resource type for which the lookup key is specified.
Select a data class	Lets you select the data class that contains the value you want to use as the lookup key.
Use in Key	Check boxes for specifying the lookup key.

- 5 Click **Save changes**.

Running a data transfer rule as a task

You can run a data transfer rule as a task. Running a rule as a task allows the rule to run with several other tasks that are included in a single job.

This task is a step in the process for importing and exporting data.

See [“Importing and exporting data”](#) on page 408.

To run a data transfer rule as a task

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, right-click the folder where you want the task to be added, and click **New > Job or Task**.
- 3 In the left pane of the **Create New Task** dialog box, click **Server Tasks > Run Connector Rule**.
- 4 In the right pane, specify a name for the task and select a data transfer rule for the task to run.
- 5 Click **OK**.
- 6 In the right pane, specify a schedule for the rule.

See [“Configuring a schedule”](#) on page 94.

See [“Running a job or task”](#) on page 352.

For more information, click the page and then press **F1**.

Viewing data transfer summaries

You can view the results of data transfers, which can include resource counts, row counts, transfer times and dates, and data source, through predefined reports. These reports can be useful in tracking data transfers.

This task is a step in the process for importing and exporting data.

See [“Importing and exporting data”](#) on page 408.

To view data transfer summaries

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, expand **Reports > Notification Server Management > Connector**, and then click the report that you want to view.

Checking the health of data transfer rules

You can check the health (proper functioning) of all the data transfer rules through predefined tasks. The health check tasks test each rule. They are the equivalent of clicking the **Test rule** option associated with each rule page for every rule.

Performing the health check helps validate that the rules and the data source definitions are configured properly. Any errors during the tests are reported and can be viewed from the Task Status for each health check task run.

The predefined tasks, like other tasks, can be scheduled to run immediately, at a specific time, or on a regular basis.

This task is a step in the process for importing and exporting data.

See [“Importing and exporting data”](#) on page 408.

To check the health of data transfer rules

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, expand **System Jobs and Tasks > Notification Server > Connector**, and then click **Connector Rules Health Check Task** or **CMDB Rule Health Check Task**.
- 3 In the right pane, specify a schedule for running the task.
See [“Adding a schedule to a policy, task, or job”](#) on page 354.
See [“Configuring a schedule”](#) on page 94.
For more information, click the page and then press **F1**.
- 4 After the task runs, go to the **Task Status** section to view the health of each of the data transfer rules.

Creating a CMDB rule to edit CMDB data

CMDB rules are the custom rules that you create for managing data and tasks. CMDB rules let you manipulate the data that is already in the CMDB. These rules let you normalize data or fix other consistency problems with your CMDB data.

You can create your own CMDB rules, where you target a group of resources based on their type and properties and then make changes to them. To create a rule, you must define the criteria for the targeted resources, the changes that occur, and the type of action to be taken. You can test the custom CMDB rules before running them in a production environment, create schedules, and notify relevant personnel. CMDB rules can also be run using tasks and jobs.

Note that the use of CMDB rules requires CMDB Solution.

Warning: CMDB rules are powerful and can alter vast amounts of data. Before you use a custom CMDB rule in a production environment, Symantec highly recommends that you test the rule by clicking the **Test rule** option on the **CMDB Rule** page.

This task is a step in the process for importing and exporting data.

See [“Importing and exporting data”](#) on page 408.

To create a CMDB rule to edit CMDB data

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Settings > Notification Server > Connector**.
- 3 Right-click **CMDB Rules**, and click **New > CMDB Rule**.
- 4 In the right pane, specify values for the rule.
For more information, click the page and then press **F1**.
- 5 Click **Save changes**.

Running a CMDB rule as a task

You can run a CMDB rule using a task, which lets you run the rule along with a series of other tasks in a job.

See [“Creating a CMDB rule to edit CMDB data”](#) on page 414.

Note: Connector Solution 6.5 user-defined tasks are not automatically migrated into the current product. You must manually re-create these tasks. Also, the ability for a task to support the running of multiple rules in a specified order has been moved to jobs. Each task can only run a single rule.

This task is a step in the process for importing and exporting data.

See “[Importing and exporting data](#)” on page 408.

To run a CMDB rule as a task

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, right-click the folder where you want the task to be added and click **New > Job or Task**.
- 3 In the left pane of the **Create New Task** dialog box, click **Server Tasks > Run CMDB Rule**.
- 4 In the right pane, specify a name for the task and select a CMDB rule for the task to run.
- 5 Click **OK**.
- 6 In the right pane, specify a schedule for running the rule.

See “[Adding a schedule to a policy, task, or job](#)” on page 354.

See “[Configuring a schedule](#)” on page 94.

Creating a virtual data class

Virtual data classes let you integrate third-party system data with the Symantec Management Platform CMDB without the need to import the data into the CMDB.

External data that is mapped to a virtual data class appears as a normal resource data class in the CMDB. Virtual data classes provide seamless integration with the Symantec Management Platform reporting features. You can use the report builder to create resource reports based on virtual data classes. The report queries the data directly from the external data source at the time you run the report.

Linked servers to these systems must initially be set up in SQL Server before you can use virtual data classes. See the Microsoft documentation about Linked Servers ([http://msdn.microsoft.com/en-us/library/ms188279\(SQL.90\).aspx](http://msdn.microsoft.com/en-us/library/ms188279(SQL.90).aspx)) for more information.

You must have the “Manage Data Connector” privilege to create, edit, or delete a virtual data class. To edit a virtual data class, you must also have Write permission on the virtual data class.

To create an editable virtual data class

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Settings > Notification Server > Resource and Data Class Settings**.
- 3 Right-click **Data Classes**, and then click **New > Virtual Data Class**.
- 4 Click **Save changes**.

Configuring data connector verbose log purging options

You can configure the purging of rule log files. Purging is performed during the standard daily schedule.

To configure data connector verbose log purging options

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Settings > Notification Server > Connector**, and then click **Connector Purge Policy**.
- 3 In the right pane, specify the rule log file purging options.
- 4 Click **Save changes**.

Security privileges and permissions

This appendix includes the following topics:

- [Security privilege categories](#)
- [Security permission categories](#)
- [Connection Profile privileges](#)
- [Management privileges](#)
- [System privileges](#)
- [Credential privileges](#)
- [Workflow Directory privileges](#)
- [Symantec Management Console privileges](#)
- [Software Management privileges](#)
- [Right-click Menu privileges](#)
- [Right-click Menu - Connector Samples privileges](#)
- [Right-click Menu - Hierarchy privileges](#)
- [Right-click Menu - Actions privileges](#)
- [Right-click Menu - Set Asset Status privileges](#)
- [Resource Management permissions](#)
- [System permissions](#)

- [Task Server permissions](#)
- [Report permissions](#)
- [Policy permissions](#)
- [Folder permissions](#)
- [Filter permissions](#)
- [Connection Profile permissions](#)
- [Credential Manager permissions](#)

Security privilege categories

A privilege allows a user to perform a particular action on the Symantec Management Platform, or on items in the Symantec Management Console. To perform an action on an item, the user's role must have the necessary permission on the item. The privileges that you can assign to a security role are grouped into categories. However, when you assign privileges to a security role, you need to select the appropriate privileges individually.

See [“Assigning privileges to a security role”](#) on page 69.

Table A-1 Security privilege categories

Privilege category	Description
Connection Profile Privileges	Lets you create and modify connection profiles. See “Connection Profile privileges” on page 421.
Management Privileges	Lets you create management items, such as filters, targets, reports, and tasks, on the Symantec Management Platform. See “Management privileges” on page 421.
System Privileges	Lets you perform management activities, such as setting up security, managing hierarchy, and importing XML files, on the Symantec Management Platform. See “System privileges” on page 423.
Credential Privileges	Lets you use the Credential Manager to create and modify credentials. These credentials are not the same as the Internal credentials and Windows credentials that are associated with user accounts. Note: The Credential Manager is a component of the extended Symantec Management Platform, so may not be installed in your environment. See “Credential privileges” on page 425.

Table A-1 Security privilege categories (continued)

Privilege category	Description
Workflow Directory Privileges	Lets you publish workflows from the workflow designer into Notification Server as a task or item action (an option on the right-click menu). See "Workflow Directory privileges" on page 426.
Console Privileges	Lets you customize the Symantec Management Console. These privileges include the ability to edit the menu, and to create portal pages, Web parts, and views. See "Symantec Management Console privileges" on page 426.
Software Management Privileges	Lets you grant specific abilities to the user role and allow the user to perform specific tasks in the Software view and Software Catalog window. These privileges also give the ability to create the Software Library and to create and import software resources. See "Software Management privileges" on page 427.
Right-click Menu Privileges	Lets you perform general actions on items in the Symantec Management Console. When you right-click on an item, the options that are relevant to that item type are available on the right-click menu. These privileges include the ability to delete an item, edit views, Web links, and item links, and start, stop, and schedule tasks. See "Right-click Menu privileges" on page 429.
Right-click Menu - Connector Samples Privileges	Examples of user-creatable right-click actions. See "Right-click Menu - Connector Samples privileges" on page 430.
Right-click Menu - Hierarchy Privileges	Lets you manage hierarchy replication. These privileges let you include or exclude specific items from hierarchy replication, and let you replicate items immediately. See "Right-click Menu - Hierarchy privileges" on page 431.
Right-click Menu - Actions Privileges	Lets you perform the actions that are relevant to the Software Management Framework. Additional solutions that are installed on the Symantec Management Platform may add further privileges to this category. See "Right-click Menu - Hierarchy privileges" on page 431.
Right-click Menu - Set Asset Status Privileges	Lets you change the status of an asset. These privileges let you set the status of a resource to Active or Retired. Solutions that are installed on Symantec Management Platform may add more privileges. See "Right-click Menu - Set Asset Status privileges" on page 433.
Right-click Menu - Time Critical Management	Lets you open the Time Critical Management page with pre-populated scope from the Computers view in the Symantec Management Console when right-clicking an organizational group, target, or filter.

Security permission categories

The permissions on an item in the Symantec Management Console determine the access that a security role has to that item. Permissions on items are applied to security roles, not to individual user accounts. For example, the Read permission on an item lets a user view it, and the Write permission on the item lets the user modify it.

See [“Assigning security permissions to folders and items”](#) on page 78.

Permissions are used with privileges to determine what actions a security role may perform on an item. For example, to delete an item a security role must have both the Delete privilege and the Delete permission on that particular item. Having only the Delete privilege, or the Delete permission on the item, is not sufficient.

You can specify the permissions that apply to each folder or item for each security role. Permissions that are applied directly to a folder or item (non-inherited permissions) are combined with the permissions that are inherited from the parent folder. The combined permissions determine the access that the security role has to that particular folder or item.

By default, child items and folders inherit all permissions on a folder. You can modify permission inheritance to suit your requirements.

Security permission categories lists and describes the categories of security permissions that you can set for each role.

Table A-2 Security permission categories

Permission category	Description
Resource Management	These permissions apply to resources. See “Resource Management permissions” on page 434.
System	These permissions apply to the system, such as reading, writing, and deleting items. See “System permissions” on page 434.
Task Server	These permissions apply to Task Server. See “Task Server permissions” on page 435.
Report	These permissions apply to reports. See “Report permissions” on page 435.
Policy	These permissions apply to policies. See “Policy permissions” on page 436.
Folder	These permissions apply to folders. See “Folder permissions” on page 436.

Table A-2 Security permission categories (*continued*)

Permission category	Description
Filter	These permissions apply to filters. See “Filter permissions” on page 436.
Connection Profile	These permissions let you use connection profiles. See “Connection Profile permissions” on page 437.
Credential Manager	These permissions let you use the Credential Manager. See “Credential Manager permissions” on page 437.

Connection Profile privileges

Connection Profile privileges let you create and modify connection profiles. Connection profiles store the information that is required to communicate with computers and other network devices using standard network monitoring protocols. These protocols include SNMP, WMI, WSMAN, and several others.

See [“Security privilege categories”](#) on page 418.

See [“Assigning privileges to a security role”](#) on page 69.

Table A-3 Connection Profile privileges

Privilege	Description
Create Connection Profile	Lets you create and modify connection profiles.

Management privileges

Management privileges let you create management items, such as filters, targets, reports, and tasks, on the Symantec Management Platform.

See [“Security privilege categories”](#) on page 418.

See [“Assigning privileges to a security role”](#) on page 69.

Table A-4 Management privileges

Privilege	Description
Create Agent Settings	Lets you create a new targeted agent settings policy, or clone an existing policy. The targeted agent settings are the general parameters that control the Symantec Management Agent, including how the agent communicates with Notification Server. See "Configuring the targeted agent settings" on page 237.
Create Automation Policies	Lets you create new automation policies. An automation policy is dynamic and specifies automated actions to perform on the Notification Server computer. It targets the appropriate computers when the policy is activated and performs whatever action is required based on the current state of each target computer. See "About automation policies" on page 327.
Create Filters	Lets you create new resource filters. A resource filter, usually known as a filter, is a dynamic definition of a set of resources. Filters are used with organizational groups to identify the resources (a resource target) that a task or policy applies to. See "About resource filters" on page 297.
Create Jobs or Tasks	Lets you create a new job or task, or clone an existing job or task. Jobs can contain multiple tasks, multiple tasks, and multiple conditions, which gives you great flexibility in setting up the job sequence that you need. See "Creating a task" on page 350. See "Creating a job" on page 350.
Create Maintenance Windows	Lets you create a new maintenance window policy, or clone an existing policy. A maintenance window is a scheduled time and duration when maintenance operations may be performed on a managed computer. A maintenance window policy defines one or more maintenance windows.
Create New Client Job	Lets you create a new client job. Client jobs are deployed to managed computers by a task server. The managed computer then runs the job and reports back to Notification Server. See "Creating a job" on page 350.
Create New Server Job	Lets you create a new server job. Server jobs run on Notification Server. See "Creating a job" on page 350.
Create Organizational Groups	Lets you create new organizational views and groups. An organizational view is a hierarchical grouping of resources (as organizational groups) that reflects a real-world structure or view of your organization.

Table A-4 Management privileges (*continued*)

Privilege	Description
Create Reports	Lets you create a new report, or clone an existing report. See “Creating and modifying custom Notification Server reports” on page 378.
Create Resource Targets	Lets you create new resource targets. A resource target, usually known as a target, is a framework that lets you apply tasks and policies to a dynamic collection of resources. A target consists of at least one organizational view or group, and a number of filters. The filters refine the available resources to identify those that you want. See “About resource targets” on page 312.
Discovery Task Management	Lets you perform Network Discovery tasks.

System privileges

System privileges let you perform management activities, such as setting up security, managing hierarchy, and importing XML files, on the Symantec Management Platform.

See [“Security privilege categories”](#) on page 418.

See [“Assigning privileges to a security role”](#) on page 69.

Table A-5 System Privileges

Privilege	Description
Change Security	Lets you change the security configuration on the Symantec Management Platform. You can create security roles, assign privileges and user accounts to security roles, and assign permissions to management items for each role. See “Setting up Symantec Management Platform security” on page 62.
Create CMDB Rules	Lets you create CMDB rules in Data Connector. You use Data Connector to transfer data between the CMDB and a data source, and manipulate data within the CMDB. Data Connector is part of the extended Symantec Management Platform. See “About Data Connector” on page 405.

Table A-5 System Privileges (*continued*)

Privilege	Description
<p>Edit SQL Directly</p>	<p>Lets you create or modify SQL queries in reports and filters. This privilege also lets you edit the data source query and view the query results of a Raw SQL Query data source for an automation policy.</p> <p>If a user is proficient in SQL and familiar with the CMDB, this privilege lets them write very specific, efficient reports. However, it can also be used to avoid security checks. For example, a user can write a query that accesses the resources that are outside their scope. That is, the resources are not contained in the organizational groups that the user has permission to view.</p> <p>Warning: Poorly written SQL queries can return incorrect results or be inefficient, consuming excessive memory and CPU time on the CMDB computer. Also, a malicious SQL query can delete, modify, or add data anywhere in the CMDB. Therefore, this privilege is very security sensitive and is only granted to the Symantec Administrators role by default.</p> <p>If you let security role members edit SQL directly, you should use the report-specific application credentials to force reports to use an account with restricted CMDB access. See “Defining an SQL query for a custom report” on page 382.</p>
<p>Import/Export XML</p>	<p>Lets you import items and resources from specially structured XML files, and export items and resources to XML files.</p> <p>Take care when you create an item or resource in the Symantec Management Platform by importing the information that is stored in an XML file. Creating an item this way bypasses all security checks.</p> <p>For example, a user can create a report by importing its XML even when the user does not have the necessary privileges and permissions. In this example the user needs the Create Reports privilege and the Create Children permission to the folder in which the report is stored.</p> <p>This privilege is very security sensitive. By default, it is granted only to the Symantec Administrators role and should not be granted to non-administrators. See “Saving console elements as XML files” on page 37.</p>
<p>Manage Data Connector</p>	<p>Lets you manage Data Connector. Data Connector is part of the extended Symantec Management Platform.</p> <p>You use Data Connector to transfer data between the CMDB and a data source, and manipulate data within the CMDB.</p> <p>See “About Data Connector” on page 405.</p>

Table A-5 System Privileges (continued)

Privilege	Description
Manage Hierarchy Replication	<p>Lets you create and run hierarchy replication rules. The hierarchy replication rules specify what is replicated to the parent Notification Server and to any child Notification Servers.</p> <p>This privilege also lets you access the standalone replication rules.</p> <p>See “Configuring hierarchy replication rules” on page 134.</p>
Manage Hierarchy	<p>Lets you add your Notification Server to a hierarchy, or remove it from a hierarchy. You can add your Notification Server to a hierarchy as a child of an existing remote Notification Server, or as its parent. Remember that your Notification Server is the one that you are logged into, which may be a remote logon.</p> <p>You require this privilege on both Notification Servers to create or change a hierarchical relationship between them.</p>
Take Ownership	<p>Lets you take ownership of a security entity. This privilege grants the new owner full permissions on the entity. For example, you would need to take ownership if all permissions on the entity were accidentally removed.</p> <p>See “Taking ownership of a folder or item” on page 87.</p>
View Security	<p>Lets you view the security configuration on the Symantec Management Platform. This information includes details of the security roles, and the user accounts, privileges, and permissions that are assigned to each role.</p>

Credential privileges

Credential privileges let you create new credentials in Credential Manager. Credential Manager provides a secure storage location for user names and passwords. The types of credentials that the Credential Manager stores are defined by the solutions that are installed on Symantec Management Platform.

See [“Security privilege categories”](#) on page 418.

See [“Assigning privileges to a security role”](#) on page 69.

When a credential is created, only the creator is granted access. If other users need to perform a management operation that requires a credential, you need to assign this privilege to the appropriate user account or role that contains the user account.

Table A-6 Credential privileges

Privilege	Description
Create Credential	Lets you create and modify credentials in Credential Manager.

Workflow Directory privileges

Workflow Directory privileges let you publish workflows from the workflow designer into Notification Server as a task or item action (an option on the right-click menu).

Workflow Server is part of Workflow Solution which is included in the Symantec Management Platform. Workflow Solution adds a page to the Symantec Management Console that lets you download and install the Workflow Designer.

See [“Security privilege categories”](#) on page 418.

See [“Assigning privileges to a security role”](#) on page 69.

Table A-7 Workflow Directory privileges

Privilege	Description
Register/Unregister Workflows	Lets you publish workflows from the workflow designer into Notification Server as a task or item action (an option on the right-click menu). For more information, refer to the Workflow solution documentation.

Symantec Management Console privileges

Symantec Management Console privileges let you customize the Symantec Management Console. These privileges include the ability to edit the menu, and to create portal pages, Web parts, and views.

See [“Security privilege categories”](#) on page 418.

See [“Assigning privileges to a security role”](#) on page 69.

Table A-8 Symantec Management Console privileges

Privilege	Description
Create Portal Pages	<p>Lets you create new portal pages. A portal page is a Symantec Management Console page that you can customize to suit your requirements. You can use a portal page to consolidate key information into a single, easy-to-view page. A portal page can display the status of the Symantec Management Platform and managed computers, or any other information that you want to make available. For example, you can include external Web pages, intranet pages, RSS feeds, or your own applications.</p> <p>You need to have the Create Children permission on the folder in which you want to create the new portal page.</p>
Create Web Parts	<p>Lets you create new Web parts. Web parts are the mini Web pages that you can use as the building blocks for portal pages. A Web part can display a report or the contents of a Web page .</p> <p>You need to have the Create Children permission on the folder in which you want to create the new Web part.</p> <p>See “Creating and modifying Web parts” on page 36.</p>
Create Views	<p>Lets you create new views. A view is a two-pane layout with a navigation tree in the left pane and content in the right pane. The navigation tree contains links to Symantec Management Console items and lets you group items from different parts of the console into a suitable structure. An item may appear multiple times in a view, and in any number of different views. A view can include folders, item links, and Web links.</p>
Edit Console Menu	<p>Lets you customize the Symantec Management Console menus. The menu options that are supplied with the Symantec Management Platform are read-only and cannot be modified. You can add new submenus, and can modify them as necessary. You can move or delete any menu item, except those that have been designated as read-only.</p> <p>See “Customizing the console menu” on page 29.</p>

Software Management privileges

Each **Software Management** privilege grants specific abilities to the user role and allows the user to perform specific tasks in the **Software** view and **Software Catalog** window from the enhanced console views. These privileges also give the ability to create the Software Library and to create and import software resources. These **Software Management** privileges are not by default part of any user role. You must assign the relevant privilege to a user role.

See [“Security privilege categories”](#) on page 418.

See [“Assigning privileges to a security role”](#) on page 69.

Table A-9 Software Management privileges

Privilege	Description
Create software products and Define software product inventory filters	<p>This privilege allows the user to use the Newly Discovered Software saved search in the Software view to find newly discovered software.</p> <p>This privilege allows the user to use the Newly discovered / undefined software and Unmanaged software panes in the Software Catalog to manage software.</p> <p>To have these abilities, you must assign the user role both the Create software products and Define software products privileges.</p>
Create software products	<p>This privilege allows the user to use the Add Product button to open the Software Product dialog box.</p> <p>This privilege also allows the user to input data into the Name, Company, Version, and Category areas of the Software Product dialog box to create software products.</p> <p>If you do not assign this privilege to the user role, the user is unable to enter information into the Name, Company, Version, and Category areas of the Software Product dialog box.</p>
Define software product inventory filters	<p>This privilege allows the user to use the Identify Inventory tab to define software product inventory filters.</p>
Configure software usage tracking	<p>This privilege allows the user to use the Add program files hyperlink and Meter / track usage tab to configure software usage tracking.</p>
Create software licenses	<p>This privilege allows the user to use the Manage Licenses button to create software licenses.</p>
Manage Software Resources	<p>Lets you create, import, edit, and delete software resources.</p> <p>A software resource is the metadata that describes a specific instance of a software product. A software resource provides a common way to describe the software so that all software-related actions can identify it accurately.</p> <p>Typically, you should give software resource privileges to the user accounts who deliver and manage software. The Symantec Software Librarian and Asset Manager security roles has this privilege by default.</p>
Manage Software Library Settings	<p>Lets you create and edit the Software Library Settings.</p> <p>The Software Library is the physical directory location of the package files that are associated with the software in the Software Catalog. Because the Software Library is a repository of the definitive, authorized versions of the packages, you should restrict library access to maintain its integrity.</p> <p>The Symantec Software Librarian and Asset Manager security roles has this privilege by default.</p>

Table A-9 Software Management privileges (*continued*)

Privilege	Description
Create software deliveries	Lets you create software deliveries (Quick Delivery or Package Delivery tasks and Manage Software Delivery policy) for selected software resource from the available software list. This privilege also allows the user to use the Delivery tab to create software deliveries.

Right-click Menu privileges

The Right-click Menu privileges (sometimes referred to as item action privileges) let you perform general actions on items in the Symantec Management Console. When you right-click on an item, the options that are relevant to that item type are available on the right-click menu. These privileges include the ability to delete an item, edit views, Web links, and item links, and start, stop, and schedule tasks.

See “[Security privilege categories](#)” on page 418.

See “[Assigning privileges to a security role](#)” on page 69.

Table A-10 Right-click Menu privileges

Privilege	Description	Applies to Item Types	Additional Requirements
Add to organizational group	Lets you add a resource to an organizational group. See “ Creating and configuring an organizational group ” on page 290.	All resources	Write permission on the organizational group.
Clone	Lets you clone an item.	All item types	Clone permission on the item.
Delete	Lets you delete an item.	All item types	Delete permission on the item.
Edit Item Link	Lets you modify an item link.	Item links only.	Write permission on the item link.
Edit Rule	Lets you edit an inventory rule.	Inventory rules only.	Write permission on the inventory rule.
Edit View	Lets you edit a view. See “ Creating and modifying views ” on page 32.	Views only.	Write permission on the view.
Edit Web Link	Lets you modify a Web link.	Web links only.	Write permission on the Web link.

Table A-10 Right-click Menu privileges (*continued*)

Privilege	Description	Applies to Item Types	Additional Requirements
Push Policy	Lets you immediately push a policy to required endpoint(s). Note that the policy must be enabled and the policy has to have a target. Also, endpoints must use persistent connection for communicating with Notification Server. Note: The policy is pushed to the client immediately, but it does not run immediately. The policy runs according to its schedule.	Policies only.	Write permission on the policy.
Schedule	Lets you schedule a policy. See “Specifying a policy schedule” on page 326.	Policies only.	Write permission on the policy.
Schedule Task	Lets you schedule a task. You can set the task to run once at a particular time, or to repeat at regular intervals. See “Adding a schedule to a policy, task, or job” on page 354.	Tasks only.	Run Task permission on the task.
Security Role Manager	Lets you open the Security Role Manager.	All item types	Write permission on the item.
Start Task	Lets you start a task immediately. See “Running a job or task” on page 352.	Tasks only.	Run Task permission on the task.
Stop Task	Lets you stop a task immediately.	Tasks only.	Run Task permission on the task.

Right-click Menu - Connector Samples privileges

The Connector Samples privileges are examples of user-creatable right-click actions.

See [“Security privilege categories”](#) on page 418.

See [“Assigning privileges to a security role”](#) on page 69.

Table A-11 Right-click Menu - Connector Samples privileges

Privilege	Description	Applies to Item Types	Additional Requirements
Ping Computer	Lets you perform a TCP/IP ping on a computer.	Computer resources only	Read permission on the organizational group that contains the computer.

Right-click Menu - Hierarchy privileges

The Hierarchy privileges let you manage hierarchy replication. These privileges let you include or exclude specific items from hierarchy replication, and let you replicate items immediately.

See [“Security privilege categories”](#) on page 418.

See [“Assigning privileges to a security role”](#) on page 69.

Table A-12 Right-click Menu - Hierarchy privileges

Privilege	Description	Applies to Item Types	Additional Requirements
Disable Replication	Lets you prevent an item from participating in hierarchy replication. All configuration items and management items, and security roles and privileges are replicated by default. This option is available only when custom hierarchy replication rules are used. See “Setting up custom hierarchy replication” on page 137.	All item types	Manage Hierarchy Replication privilege, Write permission on the item.
Replicate Now	Lets you replicate selected data directly from a Notification Server to all its child Notification Servers without including it in a replication rule. This operation is a once-off replication that takes place immediately. See “Replicating selected data manually” on page 140.	All item types	Manage Hierarchy Replication privilege, Write permission on the item.

Table A-12 Right-click Menu - Hierarchy privileges (*continued*)

Privilege	Description	Applies to Item Types	Additional Requirements
Enable Replication	<p>Lets you allow an item to participate in hierarchy replication.</p> <p>All configuration items and management items, and security roles and privileges are replicated by default. This option is available only when custom hierarchy replication rules are used.</p> <p>See "Setting up custom hierarchy replication" on page 137.</p>	All item types	Manage Hierarchy Replication privilege, Write permission on the item.

Right-click Menu - Actions privileges

The Actions privileges let you perform the actions that are relevant to the Software Management Framework. Additional solutions that are installed on the Symantec Management Platform may add further privileges to this category.

See ["Security privilege categories"](#) on page 418.

See ["Assigning privileges to a security role"](#) on page 69.

Table A-13 Right-click Menu - Actions privileges

Privilege	Description	Applies to Item Types	Additional Requirements
Assign Type	<p>Assigns a type to an unassigned software resource in the Software Catalog.</p> <p>An unassigned software resource is one that is not categorized as a software release, an update, or a service pack.</p>	Software resources only	
Create Installed Software Filter	Creates filters to find managed computers by the software that is installed on them.	Software resources only	
Detailed Export	Exports a software resource and any of its associated resource information to a detailed XML file.	Software resources only	
Edit Command Line	Opens the selected command line for editing within the software resource editing page.	Software resources only	

Table A-13 Right-click Menu - Actions privileges (*continued*)

Privilege	Description	Applies to Item Types	Additional Requirements
Edit Package	Opens the selected package for editing within the software resource editing page.	Software resources only	
Edit Software Resource	Opens the selected software resource for editing.	Software resources only	
Import Package	Changes a package's source to the Software Library from a different source such as a directory on the server or a UNC path.	Software resources only	
Merge Company Resource	Merges the selected company resource with another company resource. This privilege is useful if you have two entries for the same company that might be spelled slightly differently, such as "Symantec" and "Symantec Corporation". You can select the items to merge and specify the appropriate name to use.		
Resolve Duplicate Software Resources	When two software resources represent the same software but have different identifiers, this dialog box lets the user associate both identifiers with one software resource.	Software resources only	

Right-click Menu - Set Asset Status privileges

The Set Asset Status privileges let you set the status of a resource to Active or Retired.

Solutions that are installed on Symantec Management Platform may add more privileges to this category. For example, Asset Management solution adds three or four privileges here.

See ["Security privilege categories"](#) on page 418.

See ["Assigning privileges to a security role"](#) on page 69.

Table A-14 Right-click Menu - Set Asset Status privileges

Privilege	Description	Applies to Item Types	Additional Requirements
Active	Sets the status of the selected resource as active.	Resources only	Write permission on the organizational group that contains the resource.
Retired	Sets the status of the selected resource as retired.	Resources only	Write permission on the organizational group that contains the resource.

Resource Management permissions

These permissions apply to resources.

See [“Security permission categories”](#) on page 420.

Table A-15 Resource Management permissions

Permission	Description
Read Resource Data	Lets you read resource data.
Read Resource Association	Lets you read resource association data.
Write Resource Data	Lets you write resource data.
Write Resource Association	Lets you write resource association data.

System permissions

These permissions apply to the system, such as reading, writing, and deleting items.

See [“Security permission categories”](#) on page 420.

Table A-16 System permissions

Permission	Description
Full Control	Lets you take full control of an item that another user owns. See “Taking ownership of a folder or item” on page 87.
Delete	Lets you delete items

Table A-16 System permissions (*continued*)

Permission	Description
Write	Lets you create or modify items.
Clone	Lets you clone an existing item.
Read	Lets you open an item and views the item contents.
Change Permissions	Lets you change permissions on items.
Read Permissions	Lets you read the permissions for an item.

Task Server permissions

These permissions apply to Task Server.

See [“Security permission categories”](#) on page 420.

Table A-17 Task Server permissions

Permission	Description
Create New Task	Lets you create new tasks.
Run Script	Lets you run a script. This permission also lets you allow scheduling the End User Notification Task . You must check this permission for Default > Computer Organizational Group in the Security Role Manager for required security role.
Run Power Control	Lets you run power control tasks.
Run Task	Lets you run tasks.
Run Control Service State	Lets you run a control service state.

Report permissions

These permissions apply to reports.

See [“Security permission categories”](#) on page 420.

Table A-18 Report Permissions

Permission	Description
Run Reports	Lets you run a report.
Save Reports	Lets you save a report.

Policy permissions

These permissions apply to policies.

See [“Security permission categories”](#) on page 420.

Table A-19 Policy permissions

Permission	Description
Apply to Resource Targets	Lets you apply resource targets to policies.
Enable Policy	Lets you enable or disable a policy.

Folder permissions

These permissions apply to folders.

See [“Security permission categories”](#) on page 420.

Table A-20 Folder permissions

Permission	Description
Create Children	Lets you add items and subfolders to a folder.

Filter permissions

These permissions apply to filters.

See [“Security permission categories”](#) on page 420.

Table A-21 Filter permissions

Permission	Description
Apply Agent Settings	Lets you change a targeted agent settings policy and apply it to a resource target.

Table A-21 Filter permissions (*continued*)

Permission	Description
Apply Software Delivery Tasks	Lets you apply software delivery tasks.

Connection Profile permissions

These permissions let you use connection profiles. Connection profiles store the information that is required to communicate with computers and other network devices using standard network monitoring protocols. These protocols include SNMP, WMI, WSMAN, and several others.

See [“Security permission categories”](#) on page 420.

Connection profiles are associated with devices during network discovery. During discovery, a connection profile is selected to define the protocols and credentials to use. When discovery completes, this connection profile is then associated with each discovered resource. When information is required, the associated connection profile is used to connect.

Table A-22 Connection Profile permissions

Permission	Description
Use	Lets you use connection profiles.

Credential Manager permissions

Credential Manager provides a secure storage location for user names and passwords. The types of credentials that the Credential Manager stores are defined by the solutions that are installed on Symantec Management Platform. These permissions let you use the Credential Manager.

See [“Security permission categories”](#) on page 420.

Table A-23 Credential Manager permissions

Permission	Description
Use	Lets you use the Credential Manager.

Symantec Management Agent

This appendix includes the following topics:

- [Recommended Symantec Management Agent data update intervals](#)
- [Symantec Management Agent for UNIX, Linux, and Mac troubleshooting commands](#)

Recommended Symantec Management Agent data update intervals

The Symantec Management Agent regularly sends basic inventory data to and receives agent configuration data from Notification Server. You can configure the intervals for these updates. The more computers you manage, the less frequently you should update the data to reduce the load on Notification Server.

See [“Configuring the targeted agent settings”](#) on page 237.

Table B-1 Recommended Symantec Management Agent data update intervals

Number of managed computers	Basic inventory	Configuration request
0 - 499	30 minutes	15 minutes
500 - 1999	8 hours	4 hours
> 2000	24 hours	8 hours

Notification Server includes an automation policy that automatically sends you an email when the update intervals are lower than the recommended values. This policy, the Scalability Check, saves you from regularly checking the update intervals as computers are added to or removed

from your network. You can turn the Scalability Check policy on or off as necessary, and set the appropriate schedule.

See [“Managing automation policies”](#) on page 330.

Symantec Management Agent for UNIX, Linux, and Mac troubleshooting commands

You can use commands for troubleshooting problems. You must execute them from within a command window on the target system. Unless you specify full path names, execute these commands from the local directory where the binary resides. Binary path locations are specified with each command.

Note: The default agent installation directory for the Symantec Management Agent is `/opt/altiris/notification/nsagent`. You can modify it in the Symantec Management Console, under **Settings > Installation Settings > Agent settings**.

See [“Installing the Symantec Management Agent for UNIX, Linux, and Mac with a manual push”](#) on page 223.

Table B-2 Symantec Management Agent commands

Purpose	Command from <code>/opt/altiris/notification/nsagent/bin</code>
Force a policy refresh.	<code>aex-refreshpolicies</code>
Send basic inventory.	<code>aex-sendbasicinv</code>
View available software package tasks with the option to execute them manually.	<code>aex-swdapm</code>
Manually uninstall the agent.	<code>aex-uninstall</code>
Check if the agent is running.	<code>aex-helper check</code>
Restart the agent.	<code>aex-helper agent restart</code>
Turn on the logging and increase the log file size to 1 GB.	<code>aex-helper debug on/off - ; /</code>
Check the current connection state of the agent.	<code>aex-helper info cem</code>

The Client Task Agent can display information about any tasks that have been assigned to the UNIX/Linux client. The following table lists useful commands for the Client Task Agent.

Table B-3 Client Task Agent commands

Purpose	Execute this command from <code>/opt/altiris/notification/ctagent/bin</code>
Bring up help on a command.	<code>aex-cta help</code>
List current tasks and their execution instances.	<code>aex-cta list</code>
List tasks that are run on the client and their GUIDs.	<code>aex-cta list --show-task-id</code>
List pending tasks.	<code>aex-cta pending</code>
Refresh agent configuration.	<code>aex-cta refresh</code>
Force re-registration with the task server.	<code>aex-cta register</code>
Get information about currently registered task server.	<code>aex-cta ts</code>
Retrieve a list of the managed delivery policies that are executed.	<code>aex-cta list</code>
Retrieve a list of the managed delivery policies and Quick Delivery tasks that are executed on the client.	<code>aex-cta list --show-all-tasks</code>
Allow the deferment of task execution on the client according to task settings.	<code>aex-swd-defer</code>

Table B-4 Software management commands

Purpose	Execute this command from <code>/opt/altiris/notification/smfagent/bin</code>
Display software management jobs and their status.	<code>aex-smf list</code>
Scan and send the software inventory.	<code>aex-smf swc --scan/--send</code>
Run or rerun a managed software delivery policy.	<code>aex-smf run [GUID]</code>

The following table lists `aex-helper` commands. The `aex-helper` is a client-side utility to help troubleshoot problems and speed up administrator tasks.

The syntax for the utility is `aex-helper [command options]`

Table B-5 `aex-helper` commands

Purpose	Command from <code>/opt/altiris/notification/nsagent/bin</code>
Register dependencies between solutions.	<code>adddep</code>
Perform various tasks with the UNIX Agent.	<code>agent</code>
Change properties of registered RC services.	<code>changerc</code>
Check if the Symantec Management Agent for UNIX, Linux, and Mac is running.	<code>check</code>
Clean items from the XML registry.	<code>clean</code>
Display help on the specified command.	<code>help</code>
Query the agent for various information.	<code>info</code>
Install and registers RC scripts.	<code>installrc</code>
Work with the agent IPC framework.	<code>ipc</code>
Create wrapper scripts and links for libraries and executables.	<code>link</code>
List objects in the agent's registry.	<code>list</code>
Query the agent for various information.	<code>query</code>
Start, stop, and list registered RC services.	<code>rc</code>
Add an object to the agent's registry.	<code>register</code>
Uninstall solutions.	<code>uninstall</code>
Uninstall RC scripts.	<code>uninstallrc</code>
Remove wrapper scripts and links for libraries and executables.	<code>unlink</code>
Remove objects from the agent's registry.	<code>unregister</code>
Upgrade the Symantec Management Agent Plug-in	<code>upgrade</code>

You can also use a client-side log file to help troubleshoot problems. To troubleshoot using this log file, use the commands in the following table.

Table B-6 Log file commands

Purpose	Command from /opt/altiris/notification/nsagent/var
Raise the logging level to debug state.	aex-helper agent -s Configuration debug_level debug
Turn off the limit of log size.	aex-helper agent -s Configuration debug_file_size 0
Return parameters to default.	aex-helper agent -s Configuration debug_level error aex-helper agent -s Configuration debug_file_size 1024

Cloud-enabled Management reference topics

This appendix includes the following topics:

- [Notification Server command line tools](#)
- [Ways to configure package servers in a mixed environment](#)
- [Effects of Cloud-enabled Management on site server functionality](#)
- [Internet gateway management scripts](#)
- [About Internet gateway load balancing](#)
- [Cloud-enabled agent installation package parameters](#)
- [Cloud-enabled agent installation package for Mac computer](#)
- [Command line switches for Windows cloud-enabled agent configuration](#)

Notification Server command line tools

The following table describes the command line tools that are available for you to use on Notification Server. You can use these tools for maintaining your Cloud-enabled Management environment.

Table C-1 Notification Server command line tools

Executable name	Description
AeXGenClientCert.exe	The client certificate generator tool lets you create the client certificates that you need. The Notification Server Agent certificate authority (CA) certificate issues these certificates.
AeXGenSiteServerCert.exe	The server certificate generator tool lets you create the server certificates that you need. The Notification Server CA certificate issues these certificates. Note: Applying a regenerated server certificate to an Internet gateway affects existing Symantec Management Agents. The existing agents cannot connect to the Internet gateway until they have received updated details of the gateway's certificate thumbprint.
AeXRevokeCertificate.exe	The certificate revocation tool. This tool lets you revoke a certificate by updating the certificate revocation list (CRL). See "Revoking a Cloud-enabled Management certificate" on page 278.

See ["Cloud-enabled Management troubleshooting and maintenance tasks"](#) on page 272.

Ways to configure package servers in a mixed environment

IT Management Suite supports a mixed environment where some site servers are internal and some site servers are Internet site servers. In a mixed environment, the Symantec Management Agent first tries to use the internal package servers. If no internal package servers are available, the agent reverts to using the Internet package servers that are behind the gateway.

Table C-2 Ways to configure package servers in a mixed environment

Configuration	Description
Assign at least one package server to each Internet Site.	<p>The Internet package servers must be able to publish HTTPS codebases. At least one Unconstrained package server needs to be assigned to each Internet Site. Other package servers on site can be configured as Constrained. This means that those cannot download packages directly from Notification Server.</p> <p>This configuration of package servers works in the following way:</p> <ol style="list-style-type: none"> 1 The unconstrained package server downloads the packages from Notification Server or from another package server outside the site. 2 The packages are distributed from the unconstrained package server to constrained package servers. 3 The packages are distributed to client computers. <p>Note: For load balancing and failover options, Symantec recommends that you configure at least two unconstrained package servers in each site.</p>

Effects of Cloud-enabled Management on site server functionality

Cloud-enabled Management has the following effects on package server and task server functionality:

Table C-3 Effects of Cloud-enabled Management on site server functionality

Effect	Description
Package servers on the internal network deliver packages to cloud-enabled agents and cloud-enabled package servers using HTTPS only.	However, the internal network package servers can still distribute packages to internal network clients using UNC or HTTP. Similarly, cloud-enabled package servers in the local site can deliver packages to cloud-enabled clients in the same local site using any protocol.

Table C-3 Effects of Cloud-enabled Management on site server functionality (*continued*)

Effect	Description
The server selection process on cloud-enabled agents and package servers changes.	<p>The server selection process for cloud-enabled agents and package servers is as follows:</p> <ol style="list-style-type: none"> 1 For cloud-enabled clients in the internal network, local package servers are used. Package servers are selected according to connection speed and the lowest number of connection errors. 2 For cloud-enabled clients outside the internal network, Internet site assigned or same site package servers are selected according to connection speed and the lowest number of connection errors. 3 When two package servers return the same number of errors, they are sorted randomly.
Additional activities are required when you delete a package server.	If you delete a package server from a computer that is added to the Internet gateway, for security reasons you must also delete the package server from the Internet gateway.
A remote task server cannot be installed on a client computer with a Cloud-enabled Management Settings policy already applied to it.	<p>However, the Cloud-enabled Management Settings policy can be applied to the client computer after the task server is installed.</p> <p>Note: Symantec does not recommend you to apply the Cloud-enabled Management Settings policy to a task server.</p>
Task servers cannot provide real-time notifications or real-time task delivery.	<p>Periodic polling is the supported mode for running tasks on cloud-enabled clients. By default the Symantec Management Agent checks for tasks every 30 minutes. You can change this setting for cloud-enabled agents by modifying the Task Update setting in the Task Agent Settings policy. You find this policy page in the Symantec Management Console, under Settings > Notification Server > Task Settings.</p> <p>See "Changing Client Task Agent settings" on page 360.</p>
The speed test for task servers is replaced with random sorting.	The Client Task Agent randomizes the list of task servers in situations where the speed test-based ordering would otherwise be used. Note that the agent ignores the speed test only when it is in cloud-enabled mode.
By default, task servers work with both cloud-enabled and local agents.	<p>Task servers that are assigned to Internet site work with agents located in the intranet and those which are cloud-enabled.</p> <p>To force cloud-enabled agents to communicate with selected task server, manually assign those agents to a given task server.</p> <p>See "Managing manually assigned agents" on page 101.</p>

Internet gateway management scripts

To help you manage and maintain your Internet gateways, a number of scripts are available in the Symantec Management Platform Internet gateway installation directory.

Table C-4 Internet gateway management scripts

Script location and name	Description
Apache\bin\GenerateCert.cmd	Regenerates the server certificate.
Apache\certs\client\UpdateCertHashes.cmd	Applies a Notification Server certificate authority (CA) certificate to the Internet gateway.
Apache\certs\crl\UpdateCrlHashes.cmd	Applies a certificate revocation list (CRL) to the Internet gateway. See “Revoking a Cloud-enabled Management certificate” on page 278.
Apache\bin\StartService.cmd	Starts the Internet gateway service.
Apache\bin\StopService.cmd	Stops the Internet gateway service.
Apache\bin\InstallService.cmd	Registers (or re-registers) the Internet gateway service in Windows Services.
Apache\bin\UninstallService.cmd	Unregisters the Internet gateway service from Windows Services.

See [“Cloud-enabled Management troubleshooting and maintenance tasks”](#) on page 272.

About Internet gateway load balancing

The Internet gateway can accept up to 20,000 connections and can support 1-60,000 endpoints.

The maximum number of clients that an Internet gateway can serve, depends on your environment. For example, shorter policy and task request intervals mean that the gateway receives more requests. A higher number of requests reduces the number of clients that the gateway can support. Another variable is the connection period that the agents require. In most cases the agent connects only for a brief time. However, when the agent downloads packages or reports inventory, a connection can last for a much longer period.

In Symantec Management Platform, the Internet gateways that have connection problems are not marked as bad and ignored. On every transfer the Symantec Management Agent tries all of the gateways on its list until it finds one that works. Depending on the nature of the issues that cause gateway failures, it is possible that a particular gateway may become overloaded. The system eventually balances itself correctly without any manual intervention.

Internet gateways do not support any manually configurable load balancing. All load balancing is done automatically.

The Symantec Management Agent iterates through all available Internet gateways choosing the next from the list for each new connection. If the connection to Internet gateway fails, the Internet gateway is blacklisted with the increasing interval starting with 1 minute up to 24 hours. The agent retries to connect to the blacklisted Internet gateway when the blacklist time expires.

This process ensures that if a new gateway is added to the system, the connection load soon rebalances itself automatically. The same automatic rebalancing occurs if a gateway has a temporary problem and goes offline.

See [“Setting up Cloud-enabled Management”](#) on page 256.

See [“About preparing the Internet gateway computer”](#) on page 260.

Cloud-enabled agent installation package parameters

You can generate a Symantec Management Agent installation package from the Symantec Management Console. You need to generate the package on the Symantec Management Platform instance that manages the installed agent. The generated installation package contains the Symantec Management Agent installer for the appropriate platform. The package also contains the certificates that the client needs to trust Notification Server.

See [“Generating and installing the Cloud-enabled Management offline package”](#) on page 269.

Table C-5 Symantec Management Agent installation package parameters

Parameter	Description
Operating System	The operating system on the client computer.
Policy	<p>The drop-down list contains all of the Cloud-enabled Management policies that are currently enabled. You need to select the Cloud-enabled Management Settings policy that applies to this cloud-enabled agent.</p> <p>The selected policy specifies the available Internet gateways that the newly installed agent can use. The list of available gateways is included with the Symantec Management Agent installation package.</p> <p>See “Configuring the Cloud-enabled Management Settings policy” on page 267.</p>

Table C-5 Symantec Management Agent installation package parameters (*continued*)

Parameter	Description
Organizational Group	<p>The organizational group to which the cloud-enabled computer belongs.</p> <p>This setting is optional. If you select an organizational group, the newly installed agent is automatically assigned to the specified organizational group when the computer comes under management.</p> <p>Note: (Windows only) If you add multiple organizational groups, the end user must select the suitable organizational group on the client computer during the offline package installation. Depending on the selected organizational group, appropriate communication profile with Cloud-enabled Management information is applied.</p> <p>You need to use an organizational group that you have created. Do not choose any of the default organizational groups. Those groups are based on resource types and are not suitable for cloud-enabled computers.</p> <p>For example, a managed service provider (MSP) may have a number of different customers and manage each customer by using a customer-specific organizational group. This setting enables each newly installed computer to be automatically assigned to the appropriate organizational group.</p>
Installation name	<p>A user-friendly name for the installation package. This name is shown on the subject line of the Symantec Management Agent certificate that is attached to the installer. This name can be used for reporting and diagnostic purposes.</p> <p>For a single computer installation, you may want to use the name of the computer or the primary user. For a package that is installed on multiple computers, you may want to use the appropriate office or department identifier.</p>
Expiry	<p>The date and time that the installation package expires. The default is 7 days after the creation time.</p> <p>You must specify a date that is at least one day later than the current (creation) date.</p>
Automate certificate distribution	<p>Defines whether the permanent certificate of an agent is issued automatically. If it is not then an administrator has to manage certificate distribution and needs to authorize each request from the Reports section of Notification Server.</p>
Limit number of agent registrations	<p>Defines how many times a permanent certificate can be issued. The certificate is issued based on the number of requests that are sent using a temporary certificate or site certificate.</p>
Sign using	<p>You also have the option to add signing to the installation package. You can choose between signing with a certificate thumbprint or signing with a certificate from file.</p> <p>Note that this parameter applies to Windows packages only.</p>
Package encryption password	<p>You must define the password that needs to be entered before the package can be installed on the client computer.</p>

Cloud-enabled agent installation package for Mac computer

The cloud-enabled agent installation package lets you install the cloud-enabled agent on a disconnected Mac computer.

See [“Generating and installing the Cloud-enabled Management offline package”](#) on page 269.

The cloud-enabled agent installation package for Mac consists of the following items:

- Shell script to perform installation, user interaction, and extraction of embedded binary data.
- Bootstrap that is extended to support password-based decryption.
- Compressed agent installation package.
- Compressed and encrypted temporary certificates and xml with installation data.

The installation package supports the following command lines:

<code>--help, -h</code>	Displays the usage information and exits immediately.
<code>-dir <dir></code>	Lets you specify the installation directory. Note that this command is not shown and processed on OS X.
<code>-pwd <pwd></code>	Lets you specify the password to decrypt the package.
<code>-reinstall</code>	Lets you reinstall the agent discarding previous settings.

The generated cloud-enabled agent installation package is placed into a compressed archive along with the interactive installer. The interactive installer asks for a password to decrypt the data and a password to get the root privileges.

The compressed archive contains the following files:

- `./Symantec_Management_Agent_Installer.pkg`
The interactive installer that asks for decryption password and installs the agent. The installer is signed with the Apple certificate and contains a bootstrap that verifies all package signatures to ensure that the external package was not replaced to run arbitrary scripts.
- `./Resources/cem_package.sh`
The installation package that runs with password command line parameter to avoid user interaction.

Command line switches for Windows cloud-enabled agent configuration

(Windows only)

You can use command line switches to configure the Symantec Management Agent for Cloud-enabled Management.

Note: After you use command line switches, you must restart the Symantec Management Agent for these settings to take effect.

Table C-6 AeXNSAgent.exe command line switches

Command line switch	Description
<code>/gw=gatewayName, port, thumbprint</code>	Specifies an Internet gateway that the Symantec Management Agent can use. See “Forcing the Symantec Management Agent to use a specified Internet gateway” on page 281.
<code>/importcert=certificateFile.pfx</code>	Adds a specified certificate to the Symantec Management Agent configuration. This command places the certificate in the Symantec Management Agent service certificate store. It also adds the certificate thumbprint to the registry.
<code>/removecert</code>	Removes the current certificate from the Symantec Management Agent configuration. This command removes the agent certificate from the Symantec Management Agent service certificate store. It also removes the certificate thumbprint from the registry.
<code>/rootca=certificateFile.cer</code>	Adds a root certificate authority (CA) certificate. This command inserts the specified certificate into the Trusted Root Certification Authorities certificate store.
<code>/cem=on</code>	Enables Cloud-enabled Management on the Symantec Management Agent by turning on secure communication.
<code>/cem=off</code>	Disables Cloud-enabled Management on the Symantec Management Agent by turning off secure communication.

Table C-6 AeXNSAgent.exe command line switches (*continued*)

Command line switch	Description
/clearcem	Clears all Cloud-enabled Management Settings from the Symantec Management Agent configuration.

See [“Cloud-enabled Management troubleshooting and maintenance tasks”](#) on page 272.

Scriptable fields for modifying Resource Import Export and CMDB rules

This appendix includes the following topics:

- [Scriptable fields for modifying Resource Import Export and CMDB rules](#)

Scriptable fields for modifying Resource Import Export and CMDB rules

When you work with Resource Import Export rules for importing resources or CMDB rules, you map or set values for the columns of the specified resource type in the CMDB. Using an expression is one of the options for setting column values. An expression lets you write some .NET scripts.

The creation of expressions is documented in the following topics:

- See [“Expression syntax”](#) on page 454.
- See [“Expression operators”](#) on page 454.
- See [“User-defined values”](#) on page 455.
- See [“String operators”](#) on page 455.
- See [“Wildcard characters”](#) on page 455.
- See [“Aggregate Types”](#) on page 455.
- See [“Expression functions”](#) on page 456.

= IN LIKE

When you create comparison arithmetic expressions, the following operators are allowed:

+ (addition) - (subtraction) * (multiplication) / (division) % (modulus)

See [“Scriptable fields for modifying Resource Import Export and CMDB rules”](#) on page 453.

User-defined values

User-defined values can be used within expressions to be compared against column values. String values should be enclosed within single quotes. Date values should be enclosed within pound signs (#). Decimals and scientific notation are permissible for numeric values. Examples: "FirstName = 'John'"; "Price <= 50.00"; "Birthdate < #1/31/ 82#".

For the columns that contain enumeration values, cast the value to an integer data type. Example: "EnumColumn = 5"

See [“Scriptable fields for modifying Resource Import Export and CMDB rules”](#) on page 453.

String operators

To concatenate a string in an expression, use the + character.

See [“Scriptable fields for modifying Resource Import Export and CMDB rules”](#) on page 453.

Wildcard characters

Both the * and % can be used in expressions interchangeably for wildcards in a LIKE comparison. If the string in a LIKE clause contains a * or %, those characters should be escaped in brackets ([]). If a bracket is in the clause, the bracket characters should be escaped in brackets. Example: [[] or []]. A wildcard is allowed at the beginning and end of a pattern, or at the end of a pattern, or at the beginning of a pattern. Examples: "ItemName LIKE '*product*'"; "ItemName LIKE '*product*'"; "ItemName LIKE 'product*'".

Wildcards are not allowed in the middle of a string. For example, 'te*xt' is not allowed.

See [“Scriptable fields for modifying Resource Import Export and CMDB rules”](#) on page 453.

Aggregate Types

You can use the following aggregate types in expressions:

Sum (Sum)

Avg (Average)

Min (Minimum)

Max (Maximum)

Count (Count) StDev (Statistical standard deviation) Var (Statistical variance)

Create an aggregate expression by using one of the functions that is listed above. For example, use Sum(Price) to create a summary of figures in a column named "Price." There is no group-by functionality, therefore, all rows display the same value in the column. If a table has no rows, the aggregate functions return a null reference.

See ["Scriptable fields for modifying Resource Import Export and CMDB rules"](#) on page 453.

See ["Convert function"](#) on page 456.

Expression functions

You can choose from the following expression functions:

- Convert
See ["Convert function"](#) on page 456.
- Len
See ["Len function"](#) on page 457.
- IsNull
See ["IsNull function"](#) on page 457.
- IIF
See ["IIF function"](#) on page 458.
- Trim
See ["Trim function"](#) on page 458.
- Substring
See ["Substring function"](#) on page 458.

See ["Scriptable fields for modifying Resource Import Export and CMDB rules"](#) on page 453.

Convert function

Converts an expression to a specified .NET Framework Type.

Syntax: `Convert(expression, type)`

Table D-1 Convert function arguments

Argument	Description
expression	Specifies the expression to convert.
type	Specifies the .NET Framework type to which the value is converted.

Example: `myDataColumn.Expression="Convert(total, 'System.Int32')"`

All conversions are valid, with the following exceptions:

- Boolean can be coerced to and from Byte, SByte, Int16, Int32, Int64, UInt16, UInt32, UInt64, String, and itself only.
- Char can be coerced to and from Int32, UInt32, String, and itself only.
- DateTime can be coerced to and from String and itself only.
- TimeSpan can be coerced to and from String and itself only.

See [“Expression functions”](#) on page 456.

Len function

Gets the length of a string.

Syntax: `Len(expression)`

Table D-2 Len function arguments

Argument	Description
expression	Specifies the string to be evaluated.

Example: `myDataColumn.Expression="Len(ColumnName)"`

See [“Expression functions”](#) on page 456.

IsNull function

Checks an expression and either returns the checked expression or a replacement value.

Syntax: `IsNull(expression, replacementvalue)`

Table D-3 IsNull function arguments

Argument	Description
expression	Defines the expression to check.
replacementvalue	Defines the value to return if expression is a null reference (Nothing).

Example: `myDataColumn.Expression="IsNull(price, -1)"`

See [“Expression functions”](#) on page 456.

IIF function

Gets one of two values depending on the result of a logical expression.

Syntax: `IIF(expression, truepart, falsepart)`

Table D-4 IIF function arguments

Argument	Description
expression	Defines the expression to evaluate.
truepart	Defines the value to return if the expression is true.
falsepart	Defines the value to return if the expression is false.

Example: `myDataColumn.Expression = "IIF(total>1000, 'expensive', 'dear')`

See [“Expression functions”](#) on page 456.

Trim function

Removes all leading and trailing blank characters like `\r,\n,\t, ' '`

Syntax: `Trim(expression)`

Table D-5 Trim function arguments

Argument	Description
expression	Defines the expression to trim.

See [“Expression functions”](#) on page 456.

Substring function

Gets a sub-string of a specified length, starting at a specified point in the string.

Syntax: `Substring(expression, start, length)`

Table D-6 Substring function arguments

Argument	Description
expression	Defines the source string for the substring.
start	Specifies an integer that defines where the substring begins.
length	Specifies the integer that defines the length of the substring.

Example: `myDataColumn.Expression = "Substring(phone, 7, 8) "`

You can reset the Expression property by assigning it a null value or empty string. If a default value is set on the Expression column, all previously filled rows are assigned the default value after the Expression property is reset.

See [“Expression functions”](#) on page 456.

Glossary

Active Directory Import	A feature of the Symantec Management Platform that lets the user import Active Directory objects such as users, computers, sites, and subnets, into the CMDB (Configuration Management Database).
AeXGenClientCert.exe	A command-line tool that generates the client certificates that Cloud-enabled Management requires.
AeXGenSiteServerCert.exe	A command-line tool that generates the site server certificates.
AeXRevokeCertificate.exe	A tool that revokes certificates.
agent registration policy	A policy that lets the user automate the agent registration process. Agent registration policy is a set of rules that determine how the incoming registration requests are processed.
alert	A notification about issues, failures, and particular states of the system. The user can customize which alerts are sent, logged, and where the alerts are sent.
Alert Manager	A feature that generates a ticket when an event occurs, and sends notification messages to the designated users.
applicability rule	A rule that determines whether a computer has the correct environment for an installation of a specific software package.
application identity of Notification Server	An account under which Notification Server runs.
automated action	An action that runs in response to an event. Automated actions can generate alerts, execute tasks, create reports, and send emails.
automation policy	A rule in XML format that defines the attributes of a resource such as its groups, relationships, and wanted states. Automation policy initiates automated actions to update the resource and bring its attributes into compliance.
Basic filter	A type of filter that filters the computers according to the static parameters.
blockout period	The time when all communication between the agent and the Notification Server computer is disabled.
CEM (Cloud-enabled Management)	A feature that lets the user manage the client computers outside the corporate network without a VPN (virtual private network).
client certificate	A certificate that allows a client computer or a site server to identify itself to Notification Server.

client computer	A computer that has Symantec Management Agent installed on it and can be managed from the Notification Server computer through Symantec Management Console.
client task	A task that is executed on a client computer.
Client Task Agent	A sub-agent that runs on client computers. Client Task Agent accepts tickles from a task server and receives job and task information. It then passes this information to a handler and sends status information back to the task server. This sub-agent is installed automatically with the Symantec Management Agent.
Cloud-enabled agent	An agent that is allowed to communicate with Notification Server through an Internet gateway.
CMDB (Configuration Management Database)	The central database that stores all the data that Symantec Management Platform uses and generates.
Command-Line Builder	A tool that is used to create a syntactically correct command.
complete hierarchy replication	A process that replicates all objects and data in the hierarchy.
Complete Update schedule	A schedule that completely recreates the membership of all filters, organizational groups, and targets, regardless of inventory status or any changes to policies.
connection profile	A group of settings that defines which network protocols are used to communicate with the network devices.
Credential Manager	A secure store for the credentials that Notification Server and installed solutions use.
Data Connector	A component of the Symantec Management Platform that lets the user transfer data between external data sources and the CMDB (Configuration Management Database).
delta update schedule	A schedule that updates the membership of the filters that have had membership changes, all dynamic organizational groups, and invalid targets.
detection rule	A rule that determines if specific software is installed on a computer.
differential hierarchy replication	A process that replicates the objects and the data that have changed since the last replication.
discovery	The process of searching for computers or other resources on the network that meet specific requirements.
Documentation Library	A collection of help content that is installed with each IT Management Suite component.
event	Any action that Notification Server can monitor.
filter	A query that identifies a dynamic group of resources that share common criteria.

Full Windows Installer Repair	A policy or task that runs on client computers and verifies that all of the component resources of the Windows Installer applications are installed correctly. If any element of a component is not installed correctly, Full Windows Installer Repair initiates the repair of that component.
global exclude entry	A way to exclude application data from being saved in any application layer. Global exclude entry is used to prevent the loss of data when an application layer is reset.
hierarchy	An organizational structure of multiple Notification Servers that identifies a parent Notification Server. It then replicates the relevant data to any number of child servers, which can be located on different structural levels.
Internet gateway	A computer that tunnels communication between client computers outside the corporate network and the Symantec Management Platform infrastructure. Setting up an Internet gateway is required to use Cloud-enabled Management.
Inventory Rule Management	The software feature that lets the user create, edit, and delete rules and the expressions that make up rules.
item	Any object that belongs to CMDB (Configuration Management Database), such as a policy, a folder, or a computer that can be managed. Each item has a name, description, GUID, and attributes, and can be cloned, imported, exported, presented, and secured. Items can be linked with references or named relations between them.
job	A sequence of tasks that are executed on a target. Jobs can include the conditions that specify when the task runs.
Jobs and Tasks Portal	A page in the Symantec Management Platform that lets the user create and schedule tasks to run on the managed resources.
LAC (Legacy agent Communication)	
layer exclude entry	A way to exclude application data from being saved in a specific application layer. Layer exclude entry is used to prevent the loss of application data when an application layer is reset.
legacy agent	Symantec Management Agent that has the version that is previous to the Notification Server version. For example, in IT Management Suite 7.5 a legacy agent is Symantec Management Agent 7.1.
Legacy Software Delivery	A policy that delivers software to a client computer and is created from an earlier version of a software delivery policy.
Log Viewer	A tool that lets the user monitor several locations of logs for different components.
maintenance window	A scheduled period of time when maintenance operations may be performed on a client computer.
managed computer	A computer on which the Symantec Management Agent is installed. Another term for a client computer.

Managed Delivery	A policy that can perform complex software delivery tasks. Managed Delivery can perform recurring software deliveries, check for compliance, perform remediation, and install dependency software. It can also deliver multiple software resources and uninstall superseded software.
migration	A process of moving Symantec Management Platform data from an older platform version to a newer one. Migration is performed when the Configuration Management Database (CMDB) is not compatible with the newer version of the platform.
migration wizard	A tool that is used to perform a migration. Migration wizard is shipped with Symantec Installation Manager.
My Portal page	The default page that opens when a new user runs the Symantec Management Console.
Network Discovery	A process of discovering all IP devices that are connected to a network.
Network Discovery task	A scheduled task that discovers either a single device or multiple devices on a network.
Network Discovery wizard	A tool that is used to create a Network Discovery task.
Notification Server	The main component of Symantec Management Platform communicates with Symantec Management Agent and the CMDB (Configuration Management Database), and provides the user interface and the background that the solutions that are part of the IT Management Suite require. Notification Server processes events, facilitates communications with managed computers, and coordinates the work of the other Symantec Management Platform services.
NS Configurator	A tool that lets you change most core Notification Server configuration settings. These settings include many that are not accessible from the Symantec Management Console.
NSE (Notification Server Event)	An XML file that is transferred between Notification Server and Symantec Management Agent. NSE can contain the following information: event processing, basic or full inventory, success or failure of a package download.
offline installation package	A file that is used to install Symantec Management Agent on computers outside the corporate network. It contains an executable installation file that is generated on the Notification Server computer, and a Cloud-enabled Management policy.
organizational group	A set of resources that are grouped by common properties or similar features for management and security purposes.
organizational view	A hierarchical grouping of resources that reflects a real-world structure of an organization.
package	A file that is intended for installation on client computers.
Package Delivery task	A task that delivers and installs the software on client computers.

package server	A type of site server that is used to distribute packages from Notification Server to client computers.
permission	An ability of a particular user or group to perform specific actions on a resource and access particular items.
policy	A set of rules that are applied to a resource or a set of resources that control the execution of automated actions. Policies can be scheduled or based on the incoming data that triggers an immediate action. Policies determine when an action should start and how the results of the action are processed.
Policy Update schedule	A schedule that updates the membership of filters that a policy uses if the policy has changed since the last update.
portal page	A customizable Symantec Management Console page.
privilege	A setting that determines the actions in the Symantec Management Console that a user or a group of users can perform.
Purge Maintenance	A script that deletes old and obsolete data from CMDB (Configuration Management Database).
Query Builder	A tool that lets the user configure the query SQL to build the filter query.
Query filter	A type of filter to which the user can add the criteria from a default filter criteria list. When the user creates a new filter, it is automatically created as a Query filter.
Quick Delivery	A task that lets the user deliver the software without the need to know which package to select or how to create the command line.
replication	A one-way transfer of data between Notification Server and a client computer or another Notification Server.
replication rules	The regulations that define the data that needs to be replicated to other Notification Servers.
report drilldown	An action that is performed when the user clicks on an item in the report results.
resource	Any item that Notification Server can track or manage, such as a user, site, installed application, computer, switch, router, or handheld device.
resource import rule	A regulation that lets the user specify the resources that should be imported from Active Directory.
Resource Manager	A feature that displays information about a resource, such as its properties and current state. Resource Manager also lets the user troubleshoot and perform actions on managed resources.
resource report	A report that lets the user drill down on a particular resource to view full details in the Resource Manager.

resource scoping	A security and resource management feature that limits the data that a user can access based on the security role membership. Resource scoping is implemented by assigning permissions to organizational groups.
resource target	A framework that lets the user apply tasks and policies to a dynamic collection of resources.
rule expression	A combination of symbols (identifiers, values, and operators) that yields a result upon evaluation. These symbols form the instructions that define the items that a rule should check the client computer for.
schedule	A set time and date when an action, for example, a task, is executed. Actions can be scheduled to execute only once or with a set interval.
security role	An organizational group that contains Symantec Management Platform users. A security role is characterized by name, permissions, and the privileges that are assigned to the role.
Security Role Manager	A console that lets administrators set permissions for security roles.
server task	A task that is executed on the Notification Server computer.
shared schedule	A schedule that a number of items, such as policies or tasks, use.
site	A group of client computers that is usually based on one or more subnets.
site server	A computer that hosts a site service. A site service is a middleware component that is used to provide packages, tasks, and PXE configuration to Symantec Management Agents. A site server can host one or more from the following site services: Package Service, Task Service, Monitor Service (RMS), and Network Boot Service (DS). Site servers are used to reduce the load on the Notification Server computer.
smart rule	A rule that determines whether a package is installed on a client computer.
Software Catalog	A catalog that contains a list of known applications and predefined software products. Software Catalog is regularly updated to include the new inventory data.
Software Library	The physical location of the software packages that are defined in the Software Catalog. The Software Library is the source of the definitive, authorized versions of the software packages.
Software Management Framework	An interface that lets the user create and manage the software resources that are in the Software Catalog, and the packages in the Software Library.
Software Management Framework	An interface that lets the user create and manage the software resources that are in the Software Catalog, and the packages in the Software Library.
Software Portal	A web-based portal that lets the user request and install software with little or no outside intervention.
solution	A product that leverages the services of the Symantec Management Platform and adds specific functionality to the platform.

solution plug-in	A piece of software that is installed on a client computer and adds functionality to the Symantec Management Agent. A plug-in provides specific functions for the solution with which it is associated.
Source Patch Update	A policy or task that updates Windows Installer applications with resilient source paths.
SQL filter	A type of filter for which the user can edit the query SQL.
standard rule	A rule that determines whether a specific software application is installed on a client computer. Standard rule expressions are static.
Symantec Management Agent	The software that is installed on the computers that you want to manage. It facilitates interactions between Notification Server and a managed computer. The agent receives requests for information from Notification Server, sends data to Notification Server, and downloads files. The Symantec Management Agent also lets you install and manage solution plug-ins that add functionality to the agent.
Symantec Management Console	A web-based user interface that lets the user manage the Symantec Management Platform and any other installed solutions.
Symantec Management Platform	The platform that provides a set of services for IT-related solutions. These services include security, scheduling, client communications and management, task execution, file deployment, reporting, centralized management, and CMDB (Configuration Management Database) services.
target	A framework that lets the user perform actions on dynamic sets of resources. A target consists of at least one organizational view and a number of filters.
task	An action that is performed on a client computer or a group of client computers. Server tasks are run on Notification Server. Client tasks are run on managed computers.
task server	A site server that distributes task information from Notification Server to client computers.
upgrade	A process of patching the IT Management Suite to the newest version. This process is performed with Symantec Installation Manager. In contrast to migration, the upgrade can use the same CMDB (Configuration Management Database).
user-based policy	A policy that is executed based on the user that is logged in on a given computer.
virtual data class	A data class that lets the user integrate third-party system data with the Symantec Management Platform CMDB (Configuration Management Database) without the need to import data to CMDB.
Windows Installer Repair	A policy or task that runs on client computers and verifies that all of the component resources of the Windows Installer applications are installed correctly. If any element of a component is not installed correctly, the policy or task initiates the repair of that component.

Index

A

- Active Directory Import
 - about 168
 - Directory Synchronization schedule 175
 - discovering computers 170
 - error log 168
 - full imports 173
 - process for using 170
 - reports 168
 - resource associations, importing 169
 - resource import rules 171
 - resource types supported 171
 - running resource imports manually 176
 - scheduling resource imports 173
 - update imports 173
- Active Directory import
 - resource discovery 162
- AeXGenClientCert.exe
 - overview 443
- AeXGenSiteServerCert.exe
 - overview 443
- AeXNSAgent.exe
 - command line switches 451
- AeXRevokeCertificate.exe
 - command line parameters 278
 - overview 443
- agent. *See* Symantec Management Agent
 - persistent connection 148
 - redirecting 248
- agent registration entries
 - purging 58
- agent registration policy
 - creating 209
- agent registration request
 - allowing 216
 - blocking 216
- agent registration status
 - report 216
- agent trust
 - accept 209
 - block 209

- agent trust (*continued*)
 - registration policy 209
 - revoking 216
- aggregate
 - types 455
- application identity
 - Notification Server 49
- archiving
 - task data 357
 - task version data 360
- ARP 184
- automation policy
 - about 327
 - action 328
 - components 328
 - creating message-based 333
 - creating scheduled 331
 - creating task 337
 - data source 328
 - deleting 330
 - evaluation rule 328
 - hierarchy 140
 - managing 330
 - modifying message-based 333
 - modifying scheduled 331
 - modifying task 337
 - performing actions on 330
 - setting evaluation rule 331, 333
 - setting security on 330
 - specifying action 336
 - specifying data source 334
 - testing 330
 - trigger 328
 - turning on and off 330
 - viewing on internal schedule calendar 95

B

- blockout period
 - viewing on internal schedule calendar 95

C

- CEM Agent IIS Website
 - settings 258
- CEM Agent Settings
 - configuring 258
- CEM certificate
 - revoking 278
- CEM package for Mac
 - structure 450
- certificates
 - report 280
 - viewing 280
- chart view, report
 - about 385
 - creating 385
 - modifying 385
- cleaning
 - task data 357
 - task schedules 359
 - task version data 360
- client job
 - creating 350
- client task
 - creating 350
- client task agent
 - settings 360
- cloud-enabled agent
 - command line switches 451
 - installing offline package 269
 - installing on disconnected computer 450
 - Internet gateway selection, forcing 281
 - troubleshooting 272
- Cloud-enabled Management
 - about 252
 - AeXNSAgent.exe command line switches 451
 - agent installation package, generating 448
 - agent installation package, parameters 448
 - command line tools 443
 - configuring Cloud-enabled Management Settings policy 267
 - Internet gateway 256
 - mixed environment 444
 - package servers 445
 - preparing site servers 254
 - preparing the environment 254
 - prerequisite activities 254
 - reports 264, 284
 - revoking certificate 278
 - site servers 445
 - Cloud-enabled Management (*continued*)
 - task servers 445
- Cloud-enabled Management Settings policy
 - configuring 267
 - disabling 267
 - enabling 267
- CMDB
 - about 56
 - command timeout 56
 - database access credentials 56
 - database name 56
 - database server name 56
 - public report credentials 56
 - purging old data 58
 - resource data history 60
 - SQL authentication 56
 - viewing 56
 - Windows authentication 56
- CMDB data
 - editing 414
- CMDB rule
 - running as task 414
- CMDB rules
 - about 414
- command line tool
 - AeXGenClientCert.exe 443
 - AeXGenSiteServerCert.exe 443
 - AeXRevokeCertificate.exe 443
- command-line troubleshooting 439
- communication profile
 - creating 247
 - editing 247
 - site server 112
 - task server 349
- Complete Update schedule
 - configuring 315
- computer
 - about discovering 163
 - configuring maintenance window 244
 - configuring Symantec Management Agent policies 235
 - discovering with Active Directory Import 170
 - discovering with Resource Discovery 164
 - global agent settings 236
 - installing Symantec Management Agent 204
 - maintenance window 244
 - manually installing Symantec Management Agent 206, 219

- computer (*continued*)
 - manually uninstalling Symantec Management Agent 233
 - methods for discovering 163
 - prerequisites for installing Symantec Management Agent 208
 - pushing Symantec Management Agent 211
 - pushing Symantec Management Agent for UNIX, Linux, and Mac 223
 - scheduled Symantec Management Agent installation 214
 - selecting for Symantec Management Agent installation 211
 - Symantec Management Agent 201
 - Symantec Management Agent data update intervals 438
 - Symantec Management Agent for UNIX, Linux, and Mac pull installation 226
 - Symantec Management Agent pull installation 213
 - Symantec Management Agent uninstallation policy 230
 - Symantec Management Agent upgrade policy 230
 - targeted agent settings 237
 - computer data
 - purging 58
 - computer report. *See* custom report
 - Configuration Management Database. *See* CMDB
 - configuration settings
 - configuring with NS Configurator 55
 - connection profile
 - about 183
 - creating 183
 - console. *See* Symantec Management Console
 - console menu
 - adding menu items 29
 - adding submenus 29
 - customizing 29
 - importing submenu from XML file 29
 - console view
 - adding components 33
 - adding item links 33
 - adding Web links 33
 - creating 32
 - modifying 32
 - context menu
 - adding command line 30
 - adding custom action 30
 - context menu (*continued*)
 - adding URL 30
 - setting substitution parameters 30
 - context-sensitive help 21
 - creating and running Network Discovery tasks
 - enabling Symantec Supervisors 192
 - credential
 - creating 88
 - editing 88
 - credential manager
 - about 88
 - CSV file
 - importing computers 211
 - saving report results 373
 - custom report
 - about 378
 - chart view, about 385
 - See also* chart view, report
 - components 376
 - converting a resource query to an SQL query 381
 - creating 378, 380
 - drilldown action, about 387
 - drilldown action, parameters 387
 - drilldown action, specifying 387
 - drilldown action, wireup 387
 - drilling into results 387
 - editing 378
 - grid view, about 386
 - See also* grid view, report
 - modifying 381
 - properties, specifying 389
 - query 381
 - See also* report query
 - report parameter
 - adding 383
 - adding advanced type 383
 - creating 383
 - modifying 383
 - report parameter, defining 383
 - resource query 381
 - SQL query 382
 - customization
 - console menu 29
- ## D
- data
 - pre-processing 409
 - data class
 - viewing event data for 364

- data class (*continued*)
 - viewing inventory data for 364
 - virtual 415
 - Data Connector
 - about 405
 - capabilities 406
 - how it works 405
 - uses 406
 - data source
 - creating a definition 410
 - specifying for automation policy 334
 - using a message for automation policy 334
 - using a report for automation policy 334
 - using a resource query for automation policy 334
 - using an SQL query for automation policy 334
 - data source definition
 - creating 410
 - data synchronization
 - hierarchy replication 134
 - hierarchy requirements 128
 - Notification Server hierarchy 127
 - replicating between Notification Servers 143
 - running hierarchy replication manually 139
 - data transfer
 - configuring 411
 - setup 408
 - summaries 413
 - data transfer rule
 - checking 413
 - running 412
 - deleting
 - task data 357
 - task version data 360
 - Delta Update schedule
 - configuring 315
 - device discovery 177
 - digital certificate 280
 - discovering network devices 178
 - discovery
 - Active Directory import 162
 - domain membership 162
 - network devices 177
 - Network Discovery 162
 - resources 162
 - documentation 21
 - accessing 27
 - domain membership
 - resource discovery 162
- ## E
- email notifications
 - configuring 50
 - encryption keys
 - export 53
 - import 53
 - synchronizing 53
 - evaluation
 - license 21
 - event data
 - viewing 364
 - export rule
 - creating 411
 - exporting data 408
 - expression
 - operators 454
 - syntax 454
- ## F
- filter
 - about 297
 - creating 300, 304
 - creating static filter from report results 373
 - dependencies 311
 - exclusions 308
 - inclusions 308
 - modifying 309
 - process for creating 298
 - query 381
 - See also* filter query
 - resource query 306
 - save data in a file 311
 - scheduling membership updates 315
 - selecting query type 305
 - SQL query 307
 - updating membership 310
 - filter data
 - exporting 311
 - saving in a file 311
 - filter query
 - about 381
 - converting a resource query to an SQL query 381
 - folder
 - setting permission inheritance 79
 - setting permissions 78
 - taking ownership 87
 - function
 - Convert 456
 - expression 456

function (*continued*)

- IIF 458
- IsNull 457
- Len 457
- Substring 458
- Trim 458

G

global site server settings

- configuring 109

grid view, report

- about 386
- creating 386
- modifying 386

H

help

- accessing 27
- context-sensitive 21

hierachy

- running tasks 345

hierarchy

- about 127
 - alert status indicator 130
 - automation policies 140
 - creating hierarchical relationships 130, 133
 - enabling replication 130
 - manually replicating selected data 140
 - modifying hierarchical relationships 133
 - process for setting up 129
 - removing a Notification Server 130
 - replication. *See* hierarchy replication
 - reports 141
 - requirements 128
 - running automation policies 140
 - setting up 129
 - task status information 345
- hierarchy replication
- complete replication 134
 - configuring 134
 - custom replication 137
 - differential replication 134
 - items 134
 - manually replicating selected data 140
 - overriding differential replication schedule 139
 - replication rules 134
 - resources 134
 - security objects 134

hierarchy reports

- updating summary data 142

HTML file

- saving report results 373

I

ICMP settings

- Network Discovery task 182

import rule

- creating 411

importing data 408

individual package service settings

- applying 113

individual site server settings

- applying 110

input parameters

- receiving 356

input properties

- receiving 356

installation settings

- Symantec Management Agent for UNIX, Linux, and Mac 222

Internet gateway

- applying certificate revocation list, script 447
- applying Notification Server certificate, script 447
- backing up 282
- configuration files 256
- configuring 262
- configuring host computer 260
- downloading installation package 261
- forcing selection on cloud-enabled agent 281
- full restore 282
- load balancing 447
- log files 256
- managing 447
- overview 256
- partial restore 282
- port 262
- preparing 260
- process for installing 256
- regenerating server certificate, script 447
- registering Internet gateway service, script 447
- reporting 264
- running installation package 261
- setting up 256
- starting Internet gateway service, script 447
- status 264
- stopping Internet gateway service, script 447
- unregistering Internet gateway service, script 447

- item
 - setting permissions 78
 - taking ownership 87

J

- job
 - running 352
 - schedule 354
 - sequencing 347
 - when to use 345
- jobs
 - management 138

K

- Key Management System
 - synchronizing 53
- KMS
 - synchronizing 53
- KMS encryption keys
 - backing up 54

L

- legacy agent communication
 - disabling 49
 - enabling 49
- legacy report data
 - purging 58
- license
 - evaluation 21
 - solutions 21
- Log Viewer
 - opening 52

M

- maintenance window
 - configuring policy 244
 - viewing on internal schedule calendar 95
- maximum thread count
 - network discovery 179
- menu item
 - adding to console menu 29
 - exporting 29
 - importing 29
- message
 - data source for automation policy 334
- MIB files
 - import 199

- My Portal page
 - about 28

N

- network devices
 - delegating discovery tasks 188, 191–192, 195, 198
 - letting other users discover 188
- Network Discovery 177–178, 180–181
 - about 162
 - configuration 179
 - delegating tasks 188, 191, 195–196, 198
 - maximum thread count 179
 - methods 184
 - process 178
 - process for delegating tasks 188
 - reports 187
 - results 186
 - selecting network range 185
 - settings 179
 - task 181
 - wizard 178
- network discovery
 - delegating discovery tasks 196
- Network Discovery task
 - connection profile 182
 - creating 180–181
 - location 180–181
 - modifying 181
 - protocol settings 182
- Network Discovery tasks
 - delegating 192
 - enabling Symantec Supervisors to create 192
- Network Discovery wizard 180
- Notification Server
 - about 45
 - application identity 49
 - Configuration Management Database 56
 - configuration overview 46
 - configuration procedure 47
 - configuration settings overview 47
 - configuration types 46
 - configuring to use HTTPS 254
 - configuring with NS Configurator 55
 - creating hierarchical relationships 130, 133
 - email address settings 50
 - filter. *See* filter
 - functions 45
 - hierarchy 127

Notification Server *(continued)*

- internal schedule calendar 95
- NSE processing 49
 - See also* NSE processing
- overview 20
- package server 112
 - See also* package service
- persistent connection 148
- policies. *See* policy
- processing settings 49
- proxy server configuration 52
- replication 143
- schedule usage 89
- schedules 91
 - See also* schedule
- shared schedules 93
- site. *See* services
- site server. *See* site server
- site services 97, 112
 - See also* site service
- status message logging 51
- subnet. *See* subnet
- viewing log file 52
- viewing status messages 52

Notification Server hierarchy. *See* hierarchy

Notification Server replication. *See* replication

Notification Server resources. *See* resources

NS Configurator

- about 55

NS core settings

- backing up 54

NS registry

- backing up 54

NSE processing

- configuration settings 49
- enabling manually 49

O**organizational group**

- about 290
- adding computers 290
- adding resource to 365
- adding resources 290
- adding users 290
- assigning security roles 292
- editing a group 290
- managing 291
- performing actions on members 291
- setting custom security permissions 292

organizational group *(continued)*

- setting resource management permissions 292
 - setting system permissions 292
 - setting task server permissions 292
 - update schedule 315
 - use in resource security 286
 - viewing resources 291
- organizational view**
- about 288
 - creating 288
 - Default view 288
 - filtering groups displayed 288
 - modifying 288
 - use in resource security 286
- organizational views**
- viewing discovered devices 186
- organizational views and groups**
- creating 289
 - populating 289

P**package**

- Symantec Management Agent 233

package distribution points

- specifying credentials 53
- updating 318

package server

- individual settings 113

Package Server for inux

- configuration examples 121

Package Server for Linux 115

- about 115
- about configuring HTTPS and HTTP 120
- about configuring with the Apache Web Server 118
- about integrating Apache Web Server 116
- detecting the Apache Web Server 117
- supported platforms 115

package servers

- configurations 444

package service

- configuring settings 113
- setting as unconstrained 113

package, software

- configuration settings 317
- enabling access from UNC path 318
- updating distribution points 317–318

parameters

- input 356

- permissions
 - about 420
 - assigning to security role 78
 - connection profiles 437
 - credential management 437
 - filters 436
 - folders 436
 - how to view 86
 - permission categories 420
 - policies 436
 - reports 435
 - resource management 434
 - system 434
 - task server 435
 - persistent connection
 - about 147
 - agent 247
 - enable 49, 147, 247
 - enabling 148
 - Notification Server 49
 - ping 184
 - policy
 - about 320
 - automation policies 327
 - See *also* automation policy
 - depending on filter 311
 - global agent settings 236
 - hierarchy automation policies 140
 - maintenance window policy 244
 - managing 321
 - message-based automation policy 333
 - Policies view 321
 - real time push 321
 - schedule 354
 - scheduled automation policy 331
 - scheduling 326
 - Symantec Management Agent uninstallation 230
 - Symantec Management Agent upgrade 230
 - target 312
 - target, specifying 322
 - targeted agent settings 237
 - types 320
 - user-based 320
 - viewing on internal schedule calendar 95
 - when to use with tasks and jobs 345
 - Policy Update schedule
 - configuring 315
 - portal page
 - about 34
 - portal page (*continued*)
 - creating 34
 - modifying 34
 - My Portal 34
 - prerequisites
 - Symantec Management Agent for UNIX, Linux, and Mac installation 221
 - Symantec Management Agent installation 208
 - privilege, security
 - asset status item 433
 - assigning to security role 69
 - categories 418
 - connection profile 421
 - connector samples 430
 - credential 425
 - custom hierarchy replication 137
 - hierarchy 431
 - management 421
 - right-click action 429
 - software management action 432
 - solution-specific action 432
 - Symantec Management Console 426
 - system 423
 - workflow directory 426
 - properties
 - input 356
 - protocol settings
 - Network Discovery task 182
 - proxy server
 - configuring 52
 - purge now 58
 - push policy 321
- ## Q
- Query Builder
 - using for filter query 306
- ## R
- redirecting
 - agent 248
 - Release Notes 21
 - removing
 - task schedules 359
 - replication
 - about 143
 - complete 143
 - configuring 144
 - creating replication rules 144

- replication *(continued)*
 - deleting replication rules 144
 - differential 143
 - enabling replication rules 144
 - events 144
 - hierarchy. *See* hierarchy replication
 - items 144
 - jobs 138
 - replication rules 144
 - resources 144
 - running replication rules 144
 - security 144
 - standalone 143
- replication rules
 - hierarchy replication 134
 - replication 144
- replication server
 - managing 146
- report
 - about 367
 - chart view, selecting 370
 - creating. *See* custom report
 - customizing. *See* custom report
 - data source for automation policy 334
 - drilling into results 371
 - extracting results 369
 - grid view, selecting 370
 - hierarchy reports 141
 - modifying. *See* custom report
 - performing actions on result items 371
 - printing results 371
 - process for using 368
 - saving as Web part 375
 - saving results as a static filter 373
 - saving results to a file 373
 - saving snapshot 374
 - selecting snapshot 369
 - specifying user parameters 369
 - Symantec Management Agent installation
 - status 215
 - viewing results 370
- report data snapshot
 - purging 58
- report query
 - about 381
 - converting a resource query to an SQL query 381
 - report parameter
 - adding 383
 - adding advanced type 383
- report query *(continued)*
 - report parameter *(continued)*
 - creating 383
 - modifying 383
 - report parameter, defining 383
 - resource query 381
 - SQL query 382
- reports
 - Cloud-enabled Management 284
- resource
 - adding to organizational group 365
- resource data
 - viewing 364
- resource data history
 - saving in CMDB 60
- resource discovery
 - about 162
 - Active Directory import 162
 - discovering computers with 164
 - domain membership 162
 - Network Discovery 162
- resource event data
 - purging 58
- resource filter. *See* filter
- resource lookup key
 - creating 411
- resource management. *See* Resource Manager
- Resource Manager
 - about 362
 - accessing 363
 - adding a resource 365
 - opening from report results 371
 - tasks 365
 - viewing data 364
 - viewing event data 364
- resource query
 - data source for automation policy 334
 - defining for filter 306
 - report parameter
 - adding 383
 - adding advanced type 383
 - creating 383
 - modifying 383
 - report parameter, defining 383
- resource report. *See* custom report
- resource scoping
 - about 293
 - filters 293
 - howto 293

- resource scoping *(continued)*
 - organizational views 293
 - targets 293
- resource security
 - about 286
 - organizational groups 290
 - organizational views 288
 - process for configuring 286
 - setting custom security permissions on
 - organizational group 292
 - setting security on organizational group 292
- resource target. *See* target
- resources
 - about 391
 - excluding from filter 308
 - filter membership updates 310
 - including in filter 308
 - scheduled filter updates 315
 - security. *See* resource security
 - selecting with a filter 297
 - viewing data class information 392
 - viewing resource association type
 - information 392
 - viewing resource type information 392
- running tasks
 - hierarchy 345

S

- schedule
 - active date range 94
 - active period 91
 - agent policy 90
 - agent task 90
 - applying to policy 326
 - components 91
 - configuring 94
 - custom 91
 - including multiple schedules 94
 - maintenance window 90
 - modifiers 91
 - resource membership updates 315
 - scheduled Symantec Management Agent
 - installation 214
 - server policy 89
 - server task 89
 - shared 91
 - time zone 91
 - trigger 91
 - uses in Notification Server 89
- schedule *(continued)*
 - viewing Notification Server schedule calendar 95
- Schedule Editor
 - opening 93
 - using 94
- scriptable fields
 - Substring 453
- security
 - about 61
 - default roles 80
 - managing 82
 - password complexity settings 83
 - password lockout settings 83
 - predefined roles 80
 - resources. *See* resource security
 - setting up 62
 - unlocking locked out credentials 85
- security role
 - adding members 75
 - asset status item privileges 433
 - assigning as a member of other roles 77
 - assigning permissions 78
 - assigning privileges 69
 - assigning to organizational group 292
 - connection profile privileges 421
 - connector samples privileges 430
 - credential privileges 425
 - custom hierarchy replication 137
 - default 80
 - hierarchy privileges 431
 - item tasks privileges 429
 - management privileges 421
 - predefined 80
 - privilege categories 418
 - resource security 286
 - right-click action privileges 429
 - setting custom permissions on organizational
 - group 292
 - setting permission inheritance on folders 79
 - software management action privileges 432
 - Symantec Management Console privileges 426
 - system privileges 423
 - taking ownership of folder or item 87
 - workflow directory privileges 426
- Security Role Manager
 - about 86
 - accessing 86
- security roles
 - about 65

- security roles *(continued)*
 - configuring 65
 - creating 65
- sequencing
 - tasks 347
- server job
 - creating 350
- server processing
 - configuration settings 49
- server task
 - creating 350
- settings
 - client task agent 360
 - task server 360
- shared schedule
 - about 93
 - creating 93
 - deleting 93
 - enabling 93
 - modifying 93
 - viewing on internal schedule calendar 95
 - viewing schedule users 93
- site
 - assigning subnet 103
 - configuring for cloud-enabled agents 265
 - creating 99
 - deleting 99
 - managing 99
 - manually assigning agents 101
 - manually assigning site server 108
 - modifying 99
 - removing site server 99
 - removing subnet 99
 - site maintenance 98
 - site server 98
 - site services 97
 - unconstrained package server 113
- site server
 - adding site services 106
 - certificates 106
 - communication profile 106, 112
 - creating 106
 - global certificates rollout 109
 - global security settings 109
 - global settings 106
 - global task service settings 114
 - individual settings 110
 - managing 106
 - manually assigning to site 108
- site server *(continued)*
 - modifying 106
 - persistent connection 148
 - removing from site 106
 - removing site services 106
 - status 106
- site server port
 - individual settings 110
- site servers
 - assigning to a site 265
 - configuring for cloud-enabled agents 265
- site service
 - configuring settings 112
- site sever certificate
 - individual settings 110
- SMTP
 - SSL connection 50
- snapshot
 - creating from report results 374
- SNMP device classification 179
- SNMP devices
 - classifying 187
- SNMP settings
 - Network Discovery task 182
- Software Library content
 - backing up 54
- Software Management Framework
 - about 20
- solutions
 - installing 21
 - license 21
- SQL query
 - data source for automation policy 334
 - defining for filter 307
 - report parameter
 - adding 383
 - adding advanced type 383
 - creating 383
 - modifying 383
 - report parameter, defining 383
- SQL report. *See* custom report
- start
 - Symantec Management Agent 202
- static filter
 - creating from report results 373
- status messages
 - logging 51
 - viewing in Log Viewer 52

- string
 - operators 455
- subnet
 - assigning to site 103
 - deleting 103
 - managing 103
 - resynchronizing 103
- Symantec Management Agent
 - about 201
 - configuring agent policies 235
 - configuring maintenance window policy 244
 - data update intervals 438
 - global settings 236
 - importing computers from CSV file 211
 - installation methods 204
 - installation package parameters 448
 - installation requirements 208
 - installation status report 215
 - installing offline package 269
 - installing on selected Windows computers 211
 - local settings 237
 - maintenance window 244
 - manual installation process 206, 219
 - manual pull installation 213
 - manually assigning to site 101
 - manually uninstalling 233
 - package 233
 - See also* Symantec Management Agent package
 - prerequisites 208
 - pushing to Windows computers 211
 - redirecting to use another Notification Server 248
 - redirecting to use HTTPS 254
 - scheduled installation 214
 - selecting computers for installation 211
 - start 202
 - targeted settings 237
 - troubleshooting 439
 - troubleshooting for Cloud-enabled Management 272
 - uninstallation methods 229
 - uninstallation policy 230
 - uninstalling 229
 - upgrade methods 228
 - upgrade policy 230
 - upgrading 228
- Symantec Management Agent for UNIX, Linux, and Mac
 - .csv template file 220
 - Symantec Management Agent for UNIX, Linux, and Mac (*continued*)
 - about 201
 - creating .csv file for computer details 220
 - installation methods 204
 - installation requirements 221
 - installation status report 215
 - installing on selected computers 223
 - manual installation process 219
 - manual pull installation 226
 - package 233
 - See also* Symantec Management Agent package
 - prerequisites 221
 - pushing to computers 223
 - simultaneous installation tasks, setting 223
 - specifying installation settings 222
 - uninstallation policy 230
 - upgrade policy 230
 - Symantec Management Agent for Windows
 - importing computers from CSV file 211
 - selecting computers for installation 211
 - Symantec Management Agent manual installation
 - selecting computers 211
 - Symantec Management Agent package
 - configuring 233
 - updating distribution points 233
 - Symantec Management Console
 - about 24
 - accessing 25
 - customizable components 28
 - customization 24
 - customizing 28
 - documentation 27
 - help 27
 - importing menu from XML file 29
 - local access 25
 - menu. *See* console menu
 - portal page. *See* portal page
 - remote access 25
 - saving elements as XML files 37
 - saving submenu as XML file 29
 - Web part. *See* Web part
 - Symantec Management Platform
 - about 19–20
 - components 20
 - introduction 19
 - security 61–62, 82

T

- target
 - about 312
 - autogenerated target, about 312, 322
 - autogenerated target, saving 323
 - depending on filter 311
 - excluding items 324
 - filtering rules 324
 - including items 324
 - named target, about 312, 322
 - selecting computers 323
 - selecting resources 323
 - selecting users 323
 - specifying for policy 322
 - update schedule 315
- task
 - automation policy action 336
 - creating for automation policy 337
 - depending on filter 311
 - modifying for automation policy 337
 - running 352
 - schedule 354
 - sequencing 347
 - specifying input parameters 336
 - target, specifying 322
 - viewing on internal schedule calendar 95
 - when to use 345
- task data
 - cleaning up 357
- task input
 - receiving 356
- task management
 - about 340
- task schedules
 - cleaning up 359
- task server
 - communication profile 349
 - deploying 348
 - scaling 348
 - settings 360
 - tickle 343
- task service
 - configuring settings 114
 - global settings 114
- task status information
 - hierarchy 345
- task version data
 - cleaning up 360

tickle

- task server 343
- Time Critical Management
 - enable 49
- troubleshooting 439

U

- update summary data
 - hierarchy reports 142
- user account
 - assigning to security roles 76
 - configuring 70
 - creating 70
 - general account details 73
 - password complexity settings 83
 - password lockout settings 83
 - setting permission inheritance on folders 79
 - unlocking locked out credentials 85
- user report. *See* custom report
- user-defined
 - values 455
- users
 - user-based policies 320

V

- verbose log
 - purging 416
- virtual data class
 - creating 415

W

- Web part
 - about using in portal pages 34
 - adding to portal page 34
 - creating 36
 - creating from report 375
 - modifying 36
 - setting default size 36
 - setting fixed height 36
 - showing report results 36
 - showing URL 36
- WebSocket connection
 - about 147
 - enable 49
- wildcard
 - characters 455

X

XML file

- exporting console elements 37
- importing console menu 29
- importing console submenu 29
- restoring console elements 37
- saving console elements 37
- saving console menu 29
- saving report results 373