Altiris™ Out of Band Management Component from Symantec User's Guide

Version 7.0

Altiris™ Out of Band Management Component from Symantec User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 7.0

Legal Notice

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/techsupp/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

Asia-Pacific and Japan	contractsadmin@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Chapter 1

Introducing Out of Band Management Component

This chapter includes the following topics:

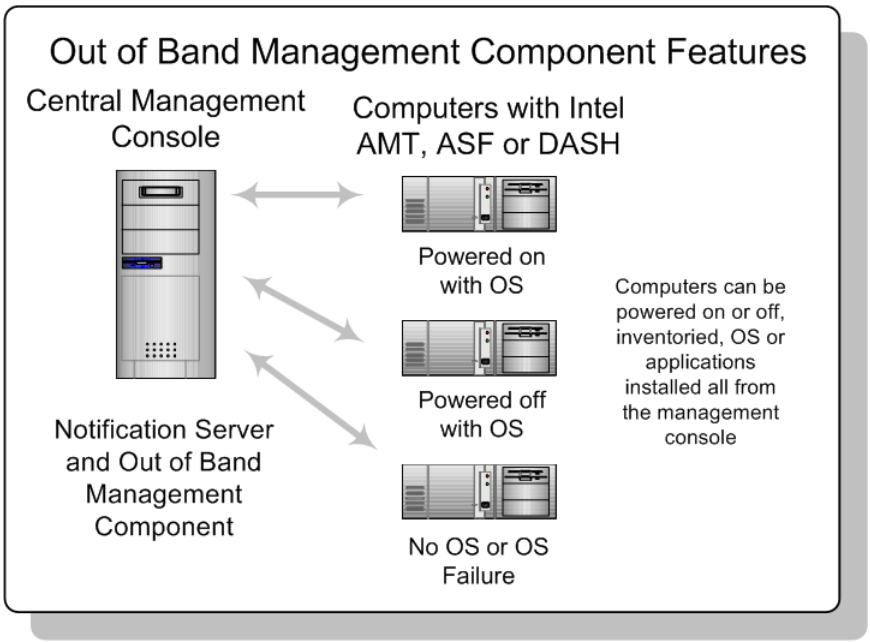
About Out of Band Management Component

Altiris Out of Band Management Component software (formerly known as Altiris Out of Band Management Solution) lets you discover computers with ASF, DASH, and Intel AMT in your environment and configure the computers for out-of-band management.

Out-of-band management is the ability to manage client computers regardless of the state of their power, operating system, or management agents. You can remotely change the power state of the computer, collect hardware inventory, and perform other management tasks that would normally require a visit to a client computer.

See "About out-of-band management" on page 10.

Figure 1-1 Out of Band Management Component features



About out-of-band management

Remote management of client computers often requires the managed computer to be turned on with an operating system running. When a computer is turned on with a running operating system, the computer is considered in-band.

Out-of-band is when a client computer is in one of the following out-of-band states:

- The computer is plugged in but is not actively running (off, standby, hibernating).
- The operating system is not loaded (software or boot failure).
- The software-based management agent is not available.

Out-of-band management is the ability to manage computers in these states. Computers with Intel AMT, ASF, or DASH capabilities can be managed out of band.

About supported out-of-band management technologies

Out of Band Management Component supports computers with the following out-of-band management technologies:

- Intel® Active Management Technology (Intel® AMT) 2.0 and later (also known as Intel® vPro and Intel® Centrino® Pro technology)
  See "About Intel AMT" on page 13.
- Broadcom ASF 2.0 and Intel ASF 2.0
  See "About ASF" on page 13.
- Broadcom DASH
  See "About DASH" on page 14.

Altiris products that can manage computers out of band

You can manage computers out of band using the following Altiris products:

- Altiris Real-Time Console Infrastructure
- Altiris Real-Time System Manager

These Altiris products let you perform the following out-of-band management tasks:

- Turn on, turn off, or restart computers.
- Configure hardware alerts and change the alerts' destination address.
- Collect the hardware information that is stored in the NVRAM of the Intel AMT device.
- Boot a computer from a remote disk or an image on a server and run the operating system repair or reinstall.
- Start a remote control session from the Symantec Management Console and enter BIOS to change settings (Intel AMT only).

What's new in Out of Band Management Component

In the 7.0 SP1 release of Out of Band Management Component, the following new features are introduced:

- An updated version of Intel SCS is installed on the OOB site server computer (by default, the Notification Server computer).
- Other minor usability and reliability improvements.

Products installed with Out of Band Management Component

When you install Out of Band Management Component, the following Altiris products are also installed.

Table 1-1 Products installed with Out of Band Management Component

Product	Description
Symantec Management Platform	The base management platform.
Altiris™ Real-Time Console Infrastructure	Provides the out-of-band one-to-many management tasks.

How Out of Band Management Component works

Out of Band Management Component installs Intel SCS on the Notification Server computer and integrates it into the Symantec Management Console. From the Symantec Management Console you can configure Intel SCS settings, discover Intel AMT capable computers, and configure them for out-of-band management.

See "About the Symantec Management Console" on page 12.

Also, Out of Band Management Component provides you with the tools to discover ASF and DASH capable computers and configure them for out-of-band management.

You can manage configured Intel AMT, ASF, and DASH computers with Altiris solutions that support out-of-band technologies.

See "Altiris products that can manage computers out of band" on page 11.

About the Symantec Management Console

The Symantec Management Console is the Web browser based administration console for working with Symantec Management Platform and solutions, including Out of Band Management Component. The console lets you perform tasks, schedule events, run reports, perform configuration, configure security, and more. You can run the console from the Notification Server computer (locally) or from a remote computer with a network connection to the Notification Server. This means you can perform administration tasks from wherever you are.

The console lets you set security that is specific to each console user. You specify which areas of the console a user has access to and the rights that a user has to

perform specific actions. For example, one user can run reports while another user can only view reports that have already been run.

You can start the console remotely by typing the following URL into the Internet Explorer's address bar: `http://<Notification_Server_name>/altiris/console`

For more information on the console, see the *Symantec Management Platform Help*, which can be accessed through the console's Help menu.

About Intel AMT

Intel Active Management Technology (Intel AMT) is a part of Intel vPro technology, which provides the following technology capabilities:

Remote manageability	Lets you remotely inventory, diagnose, and repair computers—even those that are powered off—reducing costly desk-side visits and increasing user uptime.
Security	Lets third-party security software identify more threats before they reach the operating system. You can isolate infected systems more quickly and update computers regardless of their power state.

Intel AMT is a solution that is based in hardware and firmware and is connected to the system's auxiliary power plane. Despite the power state or the operating system state of the client computer, Intel AMT provides IT administrators with access to alerts, hardware inventory, power management, circuit breaker, and agent presence functionality. Intel AMT functionality requires the computer to be plugged into the power source and connected to the network. Intel AMT functionality does not require a software agent to be installed on the client computer.

Altiris Out of Band Management Component, Altiris Real-Time Console Infrastructure, and Altiris Real-Time System Manager software support Intel AMT 2.0 and later.

About ASF

ASF (Alert Standard Format) is an industry standards-based technology that lets IT administrators manage computers regardless of the operating system state. ASF performs completely out of band and only relies on the operating system to configure the solution.

ASF provides alerting and power management functionality as long as the computer is plugged in with Ethernet connection. ASF functionality is

accomplished through hardware on the network card or system board, a software agent on the client computer, and management software on the server.

Altiris Out of Band Management Component, Altiris Real-Time Console Infrastructure, and Altiris Real-Time System Manager software support ASF 2.0.

About DASH

DASH (Desktop and Mobile Architecture for System Hardware) is a Web services-based management technology that enables IT professionals to remotely manage desktop and mobile computers from anywhere in the world, securely turn the power on/off, query system inventory, and push firmware updates among other things, regardless of the state of the remote computer.

Altiris Out of Band Management Component, Altiris Real-Time Console Infrastructure, and Altiris Real-Time System Manager software support Broadcom implementation of DASH.

What you can do with Out of Band Management Component

Out of Band Management Component helps you configure Intel AMT, ASF, or DASH devices on the computers that support these technologies, so these computers can be managed out of band.

Intel AMT tasks

Out of Band Management Component lets you perform the following Intel AMT tasks:

- Discover Intel AMT capable computers.
- Set up and configure computers with Intel AMT so that they can be managed out-of-band by other Altiris solutions.
- Define service configuration parameters for Intel SCS.
- Create the profiles that define the setup and the configuration parameters for Intel AMT, including wireless parameters.
- Manage the list of valid PID-PPS keys that match what is to be installed on the Intel AMT computers that await initialization.
- Remotely set the hostname, either detected automatically or entered manually, for an Intel AMT network interface.

- View and manage the entries that identify each Intel AMT computer that is configured or not configured.
- Remotely reset or re-configure Intel AMT computers, synchronize clocks, change power-saving policies, and so on.
- Control the list of users that have access to the Intel SCS console and to the Intel AMT devices and the permissions they have.

For more information, see the *Out of Band Management Component Implementation Guide*.

ASF tasks

Out of Band Management Component lets you perform the following ASF tasks:

- Discover ASF-capable computers.
- Install the ASF management agent on the computers.
- Collect ASF configuration inventory.
- Configure the default connection, security, and remote power control settings on client computers with ASF.
- Configure the ASF alerts that can help you be more proactive in responding to memory faults, temperature issues, hard drive warnings, chassis intrusion, and so forth. These alerts help you fix issues before they become destructive.

For more information, see the *Out of Band Management Component Implementation Guide*.

DASH tasks

Out of Band Management Component lets you perform the following DASH tasks:

- Discover DASH-capable computers.
- Install the DASH management agent on the computers.
- Collect DASH configuration inventory.
- Configure connection and security settings on client computers with DASH.

For more information, see the *Out of Band Management Component Implementation Guide*.

Where to get more information

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

Table 1-2 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues. This information is available as an article in the Altiris Knowledge Base.	http://kb.altiris.com/ You can search for the product name under Release Notes.
Implementation Guide	Information about how to install, configure, and implement this product. This information is available in PDF format.	The Product Support page, which is available at the following URL: http://www.symantec.com/business/support/all_products.jsp When you open your product's support page, look for the Documentation link on the right side of the page.
User's Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks. This information is available in PDF format.	■ The Documentation Library, which is available in the Symantec Management Console on the Help menu. ■ The Product Support page, which is available at the following URL: http://www.symantec.com/business/support/all_products.jsp When you open your product's support page, look for the Documentation link on the right side of the page.
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the Help menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ The F1 key ■ 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 Altiris products.

Table 1-3 Altiris information resources

Resource	Description	Location
Altiris Knowledge Base	Articles, incidents, and issues about Altiris products.	http://kb.altiris.com/
Altiris Juice	An online magazine that contains best practices, tips, tricks, and articles for users of Altiris products.	http://www.altiris.com/juice
Online forums	Forums for users of Altiris products.	http://forums.altiris.com/

Chapter 2

Context-sensitive topics

This chapter includes the following topics:

- Update DASH Configuration Settings task
- OOB Site Service page
- Viewing Intel SCS logs
- Integrating Intel SCS with Active Directory

Auxiliary profiles: 802.1X Profiles page

IEEE802.1X defines an extendable set of layer 2 protocols used to authenticate LAN communications. The profiles defined here can apply to any Intel AMT Profile, and to either wired or wireless connections. This capability only applies to Intel AMT releases 2.5 or later.

Note: If the Add symbol is disabled, enable Active Directory Integration on the General page.

See "General page " on page 37.

802.1X Profiles: Add 802.1x Profile dialog box

This page lets you create a new 802.1x profile.

Table 2-1 Options on the Add 802.1X Profile dialog box

Option	Description
Profile name	Type a name for the new 802.1X profile.
Protocol	Select from one of the available options.

Table 2-1 Options on the Add 802.1X Profile dialog box *(continued)*

Option	Description
Client certificate	The client authentication options require defining a source for a client certificate for authenticating an Intel AMT device to a Radius server. Type a path to a certificate authority (CA) and select a template defined for creating the appropriate client certificate. Defining a template requires an Enterprise Certificate Authority, which requires presence of Active Directory. For more information, see the *Out of Band Management Component Implementation Guide*. **Note:** Only three server and client certificates can be associated with a single profile. These include the Server certificate required for TLS and any client certificates required for 802.1x profiles or for NAC posture signing. In a normal installation, a single client certificate would be purchased for all applications in the facility. If a profile requires more than three certificates, setup of an Intel AMT device based on this profile will fail.
Roaming identity	Check to enable roaming. The user will have an identity of "Anonymous".
Trusted root CA for certificate	Select the root certificate from the Certificate Authority (CA) that was the issuer of the server certificate installed on the Radius server. Intel SCS will install a root certificate from that CA in Intel AMT devices configured with this profile.
Server certificate subject	Type the subject name in the certificate installed in the Radius server. The Full/Suffix selection below this field indicates whether this is the FQDN of the Radius server or the domain name suffix of the Radius server.

Select Certificate Generation Properties dialog box

This dialog box lets you select the certificate authority (CA) that Intel SCS uses to generate certificates.

Add Certificate Generation Properties dialog box

This dialog box lets you configure certificate generation properties.

Table 2-2 Options on the Add Certificate Generation Properties dialog box

Option	Description
CA Host Name	Type the FQDN of the computer that handles, stores, and issues digital certificates or click ... and select one from the list of Certificate Authorities (CA) known to the Notification Server. Microsoft Certificate Authority (CA) is used to generate individual certificates for Intel AMT devices.
Name	Type the name of the CA. The name is listed in the CA Administration Manager. Click the Windows Start button > Administrative Tools > Certificate Authority. The name is listed in the first sub-branch in the left pane.
Type	Windows Server 2003 Certificate Services supports two types of CAs, Enterprise and Stand-alone. The type of the CA is defined at the time of the CA installation. Select the type of the CA that you installed. For more information, see the *Out of Band Management Component Implementation Guide*.
Template	When working with an Enterprise CA, type the name of the Certificate Template to be used or click ... and select one from the list of templates known to the Notification Server. A template allows customization of the content of the certificates that are issued by the Certificate Services. The name must be the LDAP name stored in Active Directory. When the template is displayed using the CA management tools, it is the Template Name and not the Template Display Name. The default template for TLS is "WebServer". For TLS Mutual Authentication, select the template that you created for mutual. Example: "SCSUser". For more information, see the *Out of Band Management Component Implementation Guide*.

Select Certificate Template dialog box

This dialog box lets you select the certificate template that you want Intel SCS to use when generating certificates for the functionality that you are configuring.

Auxiliary profiles: Management Presence Servers page

Intel AMT 4.0 and later support CIRA (client-initiated remote access). CIRA allows a platform containing Intel AMT located outside an enterprise to connect to management consoles inside the enterprise. The connection is accomplished through a Management Presence Server (MPS) that is located in the DMZ of the enterprise. The MPS appears as a proxy server to management console applications. The Intel AMT device establishes a Mutual Authentication TLS tunnel with the MPS, and multiple consoles can interact with the Intel AMT device through the tunnel.

Click the Add symbol to add an MPS .

Management Presence Servers: Add Management Presence Server dialog box

A CIRA policy contains the parameters that determine the conditions for establishing an MPS connection, as well as the connection parameters to either one or two MPSs.

Table 2-3 Options on the Add Management Presence Server dialog box

Option	Description
Server FQDN or IP address	Type the FQDN or IP address of the Management Presence Server.
Server listening port	Type the Port that the Management Presence Server listens on for connections from Intel AMT devices.

Table 2-3 Options on the Add Management Presence Server dialog box *(continued)*

Option	Description
Client certificate	TLS mutual authentication is used to authenticate the Intel AMT-MPS tunnel. The Intel AMT device requires a client certificate that the MPS will authenticate and a trusted root certificate from the certification authority that generated the MPS server certificate. Select client certificate generation properties. Choose the Certificate Authority that the AMT platform will use to request a certificate that the MPS can authenticate and select the template that is defined for creating the appropriate client certificate. This should be a template where the subject name is supplied in the request and the usage is Client Authentication. For information on creating a template for 802.1x client certificates see the *Intel® Active Management Technology Setup and Configuration Service Installation Guide.*
Server certificate	Choose the root certificate of the Certificate Authority that the MPS will use to authenticate itself to the AMT platform.

Auxiliary profiles: Remote Access Policies page

Intel AMT Release 4.0 and later releases support CIRA (client-initiated remote access). CIRA allows a platform containing Intel AMT located outside an enterprise to connect to management consoles inside the enterprise. The connection is accomplished through a Management Presence Server (MPS) located in the DMZ of the enterprise. The MPS appears as a proxy server to management console applications. The Intel AMT device establishes a Mutual Authentication TLS tunnel with the MPS, and multiple consoles can interact with the Intel AMT device through the tunnel.

A Remove Access policy contains the parameters that determine the conditions for establishing an MPS connection, as well as the connection parameters to either one or two MPSs.

Remote Access Policies: Create Remote Policy dialog box

This dialog box lets you create a remote access policy to use with the CIRA (client-initiated remote access) functionality of Intel AMT.

See "Auxiliary profiles: Remote Access Policies page" on page 24.

Table 2-4 Options on the Remote Access Policies: Create Remote Policy dialog box

Option	Description
Name	Type a descriptive name for the policy
Tunnel life time	Type an interval in seconds. When there is no activity in an established tunnel for this period of time, the Intel AMT device will close the tunnel. Entering zero (0) means the tunnel will not time out. The tunnel will stay open until it is closed by the user or when a different policy with higher priority needs to be processed.
Trigger	Select the trigger or triggers associated with this policy. A particular trigger type can be selected in only one policy.
User initiate connection	The Intel AMT device establishes a tunnel with the MPS when the user initiates a connection request.
Alert occurred	The device establishes a connection when an event occurs that generates an alert that is addressed to the network interface.
Connect periodically	The device connects to the MPS based on the Seconds Between Connections interval.
Management Presence Servers	Select the MPSs that apply to the policy (up to two). When a trigger occurs, the Intel AMT device attempts to connect to the server that is listed in the Preferred server box. If that connection does not succeed, the device tries to connect to the server listed in the Alternative server box, if one was specified.

Auxiliary profiles: Trusted Root Certificates page

This page lists the trusted root certificates that you can use in configuration and auxiliary profiles.

Click the Add symbol to add a certificate by selecting a certificate authority found in your environment.

Click the Import symbol to import a certificate from a file.

Trusted Root Certificates: Select a Certificate Authority dialog box

Select the certificate authority (CA) that you want the solution to use when generating certificates, and click OK.

For more information, see the *Out of Band Management Component Implementation Guide*.

Trusted Root Certificates: Import Trusted Root Certificate dialog box

Import the trusted root certificate authority (CA) certificate that you want the solution to use when generating certificates, and click OK.

For more information, see the *Out of Band Management Component Implementation Guide*.

Auxiliary profiles: Wireless profiles page

A wireless profile defines which protocol will be used between an Intel AMT device and a wireless access point when the host on a mobile platform is in a Sx power state (S3, S4, or S5) and Intel AMT is configured to be active in the current power state. The profiles conform to IEEE 802.11i.

For more information, see the *Out of Band Management Component Implementation Guide*.

Wireless profiles: Add Wireless Profile dialog box

This dialog box lets you configure the wireless settings that the Intel AMT devices should use in sleep (S3, S4, or S5) state when operating system cannot be used to configure wireless protocols.

Table 2-5 Options on the Wireless profiles page: Add Wireless Profile dialog box

Option	Description
Profile name	Type a name for this profile.
SSID	Type an optional Service Set ID (SSID): a 1 to 32 character string naming a specific wireless LAN.
Data Encryption	Select a Key Management scheme (WPA or RSN) and an Encryption Algorithm (TKIP or CCMP). These choices must correspond to the settings that are used in the specific wireless LAN environment.
Authentication	Either provide a pass phrase or select one of the existing 802.1X profiles or create a new one. See "Auxiliary profiles: 802.1X Profiles page" on page 20.

Configuration profiles page

Configuration profiles contain the Intel AMT device configuration parameters. Profiles determine which features are enabled in the device, what authentication mechanism will be used, and which users have access to device features. One or many profiles can be defined. For example, use a different profile for different sites. Each profile can be assigned to one or more Intel AMT devices.

For more information, see the *Out of Band Management Component Implementation Guide*.

Setup and configuration profile: General tab

On this tab, type general information that pertains to this profile.

Table 2-6 Options on the General tab

Option	Description
Profile name	Type a short, descriptive name. This name appears on the Intel AMT devices page.
Profile description	Type a more complete description of the profile.
Max clock tolerance	Type the Max Clock Tolerance. This is the allowable difference between the clock of an Intel AMT device and the timestamp of a received message. This is part of the mechanism used to eliminate "replay" attacks.

Table 2-6 Options on the General tab *(continued)*

Option	Description
Username	The user name is always "admin".
Intel AMT 2.0 password	Select either Random Creation or Manual. If Manual is selected, type the password and confirm the entry. You must type a strong password. For more information, see the *Out of Band Management Component Implementation Guide*. The above user name and password will be the administrative user name and password in the Admin ACL entry for all Intel AMT devices that are configured with this profile. Selecting Random creation means that a random password for each Intel AMT computer that is configured with this profile will be kept in the Intel SCS database. Unless you configure more administrative users on the ACL tab, you can manage the computers from the Notification Server only. In this case, the Notification Server will pull the administrative credentials from the Intel SCS database every time you run an out-of-band task. See "Setup and configuration profile: ACL tab" on page 32. **Note:** To use the credentials that are stored in Intel SCS, select Runtime credentials profile when running a task. For more information, view topics about using connection profiles in the *Symantec Management Platform Help*.
New MEBx password	Type the new MEBx password that Intel SCS will set on devices that you initialize using the Remote Configuration feature. For more information, see the *Out of Band Management Component Implementation Guide*.

Setup and configuration profile: Network tab

On this tab, define this profile's network settings.

Table 2-7 Options on the Network tab

Option	Description
Enable ping response	When enabled, the Intel AMT device will respond to a ping.
Use VLAN	Check if you want to use a VLAN.

Table 2-7 Options on the Network tab *(continued)*

Option	Description
VLAN tag	If a VLAN is used, set the VLAN Tag, which is used to distinguish between different VLANs. **Caution:** Be careful when configuring the VLAN value. If the value is incorrect, the Intel AMT devices will not be accessible.
Web user interface	Administrators can use this browser-based interface for management and maintenance of Intel AMT devices.
Serial over LAN	This feature is used to manage an Intel AMT-enabled platform remotely by encapsulating keystrokes and character display data in a TCP/IP stream.
IDE redirection	Use this feature to remotely enable, disable, format, or configure individual floppy or IDE CD drives and to reload operating systems and software from remote locations. These actions are independent of and transparent to the host.
Wired LAN 802.1x profile	Select an optional 802.1x profile, which is used by the Intel AMT device to authenticate on a wired LAN when the device is active in S3, S4, or S5 power states. This option applies only to Intel AMT releases 2.5, 3.0, 4.0, and 5.0. See "Auxiliary profiles: 802.1X Profiles page" on page 20. **Note:** You must integrate Intel SCS with Active Directory to configure an Intel AMT device with a wired 802.1x profile. For more information, see the *Out of Band Management Component Implementation Guide*. See "Integrating Intel SCS with Active Directory" on page 59.
Keep 802.1x session after boot for PXE boot for	When selected, the 802.1x session is kept alive after a PXE Boot for the number of minutes that you specify (up to 1440 minutes). This is the period that is allowed for completion of an 802.1x authentication. This parameter can be set only when an 802.1x profile has been selected. If the 802.1x profile is deleted, this value is forced to zero.
Enable 802.1x for AMT even if host is not authorized for 802.1x	When selected, manageability traffic is enabled even if the host cannot complete 802.1x authentication to the network.

Table 2-7 Options on the Network tab *(continued)*

Option	Description
Enable Endpoint Access Control (EAC)	Choose the certificate authority and the template to use for issuing a client certificate for Endpoint Access Control (EAC) posture signing.

Setup and configuration profile: TLS tab

If you want the Intel AMT devices to require a certificate when authenticating with other applications, on the TLS (Transport Layer Security) tab, type information about the profile's certificates.

Note: You must have a properly configured infrastructure (Certificate Authority installed, proper certificates installed) to configure Intel AMT computers with TLS or TLS Mutual Authentication.

For more information, see the *Out of Band Management Component Implementation Guide*.

Table 2-8 Options on the TLS tab

Option	Description
Use TLS	When TLS is enabled, the Intel AMT device requires a server certificate that is used to authenticate itself with other applications. When Use TLS is selected, configure the interfaces to indicate which will use TLS, mutual TLS, or neither.
Local Interface	Select if the host communications with the Intel AMT device will require TLS or TLS with mutual authentication.
Network Interface	Select if network communications with the Intel AMT device will use TLS or TLS with mutual authentication.
Encryption Mode	Select Encrypted to allow setup and configuration only on platforms that support encryption. Select Plain Text to allow setup and configuration only on platforms that do not support encryption. Select Both to allow setup and configuration on both types of platforms (encrypted and plain text).

Table 2-8 Options on the TLS tab *(continued)*

Option	Description
Server Certificate	Identify the Certificate Authority (CA) associated with this profile that will be used to generate server certificates for the Intel AMT devices that are associated with the profile. See "Add Certificate Generation Properties dialog box" on page 21. **Note:** Only three server and client certificates can be associated with a single profile. These include the Server certificate that is required for TLS and any client certificates that are required for 802.1X profiles or for NAC posture signing. In a normal installation, a single client certificate would be purchased for all applications in the facility. If a profile requires more than three certificates, setup of an Intel AMT device that is based on this profile will fail.
Certificate Revocation List (CRL) (Optional)	The Certificate Revocation List (CRL) is a list of entries that indicate which certificates have been revoked. The CRL contains certificate authority URLs and the serial numbers of revoked certificates. This is an optional feature of TLS Mutual Authentication. Click the Manage CRL symbol to define a CRL.
FQDN Suffixes	The Fully Qualified Domain Name (FQDN) suffixes that will be used by mutual authentication. Type the FQDN suffix of the Notification Server computer. Example: yourenterprise.com. If you want to type more than one suffix, use a colon as a delimiter. The Intel AMT device validates that any client certificates that are used by Intel SCS or Altiris solutions have one of the listed suffixes in the certificate subject.
Trusted certificates list	These are the issuers of the client certificates that the Intel AMT device recognizes as authentic. These certificates are stored in the database and then sent to the Intel AMT device during configuration. Intel AMT can accept up to four trusted root certificates, so no more than four should be added to a profile. Click the Add symbol and, in the Select Trusted Root Certificate dialog box, select the Certificate Authority (CA) that you configured to issue certificates for TLS with Mutual. You can also click import the trusted root CA certificate from a file. For more information, see the *Out of Band Management Component Implementation Guide*.

TLS: Edit CRL dialog box

The Certificate Revocation List (CRL) is a list of entries that indicate which certificates have been revoked. The CRL contains certificate authority URLs and the serial numbers of revoked certificates. This is an optional feature of TLS Mutual Authentication.

This feature requires a Certificate Authority installed in your environment.

For more information, see the *Out of Band Management Component Implementation Guide*.

Add and select the CRL you want to use.

Edit CRL: Add CRL Entry dialog box

The Certificate Revocation List (CRL) is a list of entries which indicate which certificates have been revoked. The CRL contains certificate authority URLs and the serial numbers of revoked certificates. This is an optional feature of TLS Mutual Authentication.

Table 2-9 Options on the Add CRL Entry dialog box

Option	Description
CRL Uri	Click to select the location of the CRL you want to use.
Serial Numbers	Click the Browse symbol to select from the list of available serial numbers. Click the Add symbol to add a serial number manually.

Add CRL Entry: Select CRL Uri dialog box

This dialog box lets you select the source of the Certificate Revocation List (CRL).

Edit CRL: Import CRL dialog

This dialog box lets you import the Certificate Revocation List (CRL) from a file.

Setup and configuration profile: ACL tab

The Intel AMT access control list (ACL) manages who has access to which capabilities within Intel AMT. An ACL entry has a user ID and a list of realms to which a user has access. This access is required to use the functionality that is associated with a realm. There are two kinds of ACL entries: Kerberos and non-Kerberos. The main difference between them is that Kerberos entries have

an Active Directory SID to identify a user or group of users. Non-Kerberos entries have a user name and password for user identification. When Microsoft Active Directory is used, user identities are imported from Active Directory; otherwise, user identities are added manually.

Kerberos users are not available if AD integration is disabled.

For more information, see the *Out of Band Management Component Implementation Guide*.

See "Integrating Intel SCS with Active Directory" on page 59.

ACL: Add ACL Entry dialog box

This dialog box lets you add a user to the Intel AMT access control list (ACL).

Table 2-10 Options on the Add ACL Entry dialog box

Option	Description
Active Directory user	Select this option only if you have Active Directory integration enabled. For more information, see the *Out of Band Management Component Implementation Guide*. See "Integrating Intel SCS with Active Directory" on page 59. Select a user or group from the Active Directory.
Digest User	Digest authentication is a password-based authentication. Type the user name. Then, type the password and confirm the entry.
Realms	Select the specific functional capabilities such as Redirection or PT Administration that will be available to this ACL entry.
Access Permission	This parameter defines locations from where the user is allowed to perform an action. A user might be limited to local actions or might also be able to perform actions from the network. Select Local Access if you want the user to access the Intel AMT device through the local host only. Select Network Access if you want to let the user execute actions through the network. Select All if you want to let the user execute actions both locally or from the network. We do not recommend selecting this option.

Add ACL Entry: Select User dialog box

Select the Active Directory user you want to use for the functionality you are configuring.

Setup and configuration profile: Wireless profiles tab

You can use the Wireless profiles tab to create and select wireless profiles to use when you configure notebook computers with Intel AMT. When the Intel AMT device on a notebook computer is active in S3, S4, or S5 power states, it will attempt to authenticate according to the selected wireless profiles in order of priority. Intel SCS allows up to 15 wireless profiles to be added to a profile.

Note: An Intel AMT notebook computer configured with a wireless profile offers full Intel AMT management functionality via wireless connection, except for configuration. Configuration is possible only when the computer is connected to the wired network.

Note: If you want to use wireless profiles with 802.1X authentication to configure notebook computers with Intel AMT, you must enable Active Directory integration.

See "Integrating Intel SCS with Active Directory" on page 59.

Table 2-11 Options on the Wireless profiles tab

Option	Description
Create new wireless profile	Click to create a new wireless profile. See "Auxiliary profiles: Wireless profiles page" on page 26.
Add	Add a wireless profile.
Up/Down	Adjust the relative priority of the profile. The profile at the top of the list will have the highest priority and will be tried first by configured wireless Intel AMT devices.
Enable host VPN routing	When selected, Intel AMT devices accept management traffic over a Virtual Private Network connection when Intel AMT detects that the platform is operating outside the enterprise network.
Allow wireless connection without profile	Check to allow WiFi connection even without a profile (using the host's WiFi settings).

Setup and configuration profile: Power policy tab

Use the Power Policy settings to determine what is the highest power state when the Intel AMT devices assigned to this profile will be active or will activate from a sleep state.

Table 2-12 Options on the Power policy tab

Option	Description
AMT is ON in the following host sleep states	This parameter defines the highest power state at which Intel AMT will operate while the device is connected to AC power. Note that this includes operation in higher power states. For example, if the platform is in S3 and this parameter is set to Host is ON (S0), the Intel AMT device will not operate until the platform returns to S0. Default: Intel AMT is always on (S0-S5).
Idle timeout	Once the Intel AMT device wakes up and the host system is not turned on, this parameter determines the minimum time (in minutes) that the Intel AMT device remains operable when there is no activity. The device returns to a sleep state after the idle timeout period. The timeout timer is restarted whenever the device is serving requests. If the value of the parameter is zero (the default value), the device will remain on when there is no activity. For example, the AMT is ON parameter is set to Host is ON (S0) or in Standby (S3). When the platform transitions to S3, the Intel AMT device remains awake until there is no activity for the number of minutes set in the Idle Timeout. At that point the device reduces power. Any network access to the Intel AMT device causes it to wake up and restart the timeout timer. If you want to use this parameter, set it to three minutes at a minimum.

Setup and configuration profile: Domains tab

The Domains tab defines the domains from which an Intel AMT computer can initiate configuration by Intel SCS.

Click the Add symbol to add a domain.

If you want to allow configuration when the platform has no domain name, check Allow configuration when platform has no domain name.

Domains tab: Add New Domain Entry dialog box

Use this dialog box to add a domain to the list of domains from which an AMT computer can initiate configuration by Intel SCS.

Table 2-13 Options on the Add New Domain Entry dialog box

Option	Description
Domain name	Type the name of the domain.
This domain is a home domain	Selecting this box has the following effects: ■ CIRA (Remote access): If the Intel AMT computer is not in a home domain, the computer will attempt to use CIRA to connect to the SCS (if CIRA is defined). ■ WiFi: If the Intel AMT computer is in a home domain and no wired connection is available, and the profile does not include WiFi parameters, and the host has connected using WiFi, the Intel AMT computer will use the host's WiFi settings as long as the access point is in one of these domains.
FQDN validation	If selected, when the user sets the configuration properties for an Intel AMT device, the SCS checks that the device's FQDN matches one of the domains in the domain list of the profile that is used for setup and configuration.
Allow sub-domain	When selected, Intel SCS will allow configuration (using this profile) of an Intel AMT computer in a sub-domain of the domain that is entered in the Domain Name box. For example, if the domain name is mydomain.com, Intel AMT computers in subdomain.mydomain.com can also be configured.

Setup and configuration profile: Remote Access tab

Intel AMT 4.0 and later support client-initiated remote access. This feature allows a platform containing Intel AMT located outside an enterprise to connect to management consoles inside the enterprise. The connection is accomplished through a Management Presence Server (MPS) located in the DMZ of the enterprise. The MPS appears as a proxy server to management console applications. The Intel AMT device establishes a Mutual Authentication TLS tunnel with the MPS, and multiple consoles can interact with the Intel AMT device through the tunnel.

For remote access to work, the Intel AMT platform must first be configured by Intel SCS when it is inside the enterprise with the information needed to connect with the MPS. The Remote Access tab is used to enter the necessary parameters. A remote access policy contains the parameters that determine the conditions for establishing an MPS connection, as well as the connection parameters to either one or two MPSs.

The MPS connection parameters are defined separately.

DNS configuration page

The computer with Intel SCS installed (the OOB site server computer) must be registered in DNS as "ProvisionServer". This must be done in each DNS domain. Intel AMT devices send their hello packets to this hostname.

This page lets you test if the DNS is configured correctly.

Note: If this test fails, you cannot use the Remote Configuration feature.

For more information, see the *Out of Band Management Component Implementation Guide*.

Also, you cannot set up and configure the Intel AMT capable computers that were initialized by an OEM or with a USB key. Only computers with Intel AMT device initialized thru MEBx can be configured.

For more information, see the *Out of Band Management Component Implementation Guide*.

Table 2-14 Options on the DNS configuration page

Option	Description
Test	Click to see if DNS is configured correctly. Verify that the IP of the "ProvisionServer" matches the IP of Intel SCS.

General page

This page lets you modify general settings of the Intel AMT Setup and Configuration Service.

This page lets you modify the settings of Intel SCS selected as default on the Service Location page.

See “Service location page ” on page 43.

The default settings are adequate for normal operation of Intel SCS, however, if you want to use Active Directory users, TLS Mutual Authentication, or 802.1X profiles, you must integrate Intel SCS with Active Directory and check Integrate with Active Directory on this page.

For more information, see the *Out of Band Management Component Implementation Guide*.

See “Integrating Intel SCS with Active Directory” on page 59.

Table 2-15 Options on the General page

Option	Description
Listen Port	Each instance of Intel SCS listens for Hello messages from the Intel AMT devices on a defined TCP port. Type the TCP port used for listening. The default port is 9971.
Active Directory integration	Selecting Schema Extension or Standard will cause the Intel SCS server to add AMT objects to Active Directory. This enables the use of Kerberos authentication and the Active Directory users list. Active Directory is also required for TLS Mutual Authentication and 802.1X profiles. Before you select AD integration, you must integrate Intel SCS with Active Directory. See "Integrating Intel SCS with Active Directory" on page 59.
Require confirmation before Intel AMT configuration	When the Intel SCS receives a Hello message from an Intel AMT device, setup and configuration will proceed automatically, unless this option is checked. If you check this option, you will have to authorize setup and configuration through the Authorize systems operation on the Intel AMT Systems page. See "Intel AMT systems page" on page 45.
Allow Remote Configuration	Intel AMT releases 2.2, 2.6, 3.0, 4.0, and 5.0 support Remote Configuration. As part of this feature, the Intel AMT device sends a self-signed certificate for the TLS Mutual Authentication process. This certificate is used for setup and configuration only. The device creates the self-signed certificate just before sending the first "Hello" message. Check this option to enable Intel SCS to accept self-signed certificates from Intel AMT devices. For more information, see the *Out of Band Management Component Implementation Guide*.
Use one time password	Check to add an additional security feature. This will require a one-time password (OTP) exchange between Intel SCS and the Intel AMT device requesting setup and configuration.
First Common Name (CN) in certificate subject name	Select an option that matches your root certification authority certificate's CN field.

Table 2-15 Options on the General page *(continued)*

Option	Description
Log Level	The system wide actions log can be recorded at several levels. The more detail that is recorded, the more system resources and bandwidth must be allocated.
Service Maintenance Queue Polling Period	This parameter determines how frequently the Intel SCS checks the queue in the database. The default is 1000 milliseconds.
Max Queue Size	This parameter sets the maximum permitted length of the database queue. If the queue is full when the server or the API tries to add an additional entry, the entry will be lost. The default is 1000 requests.
Worker Threads	This parameter limits the number of Worker Threads that are permitted simultaneously. The default is 10 threads.
Keep Log For	This parameter determines how long log entries are saved. The default is 60 days.
Keep Security Audit Log For	This parameter determines how long security status entries are saved. The default is 2 months.

Select Active Directory Organizational Unit dialog box

This page lets you select the Active Directory Organizational Unit for the functionality you are configuring.

Maintenance page

This page lets you define actions that Intel SCS will perform periodically on all configured Intel AMT devices.

On this page you configure the Intel SCS that you selected as default on the Service Location page.

See "Service location page " on page 43.

The default settings are adequate for normal operation of Intel SCS.

Table 2-16 Options on the Maintenance page

Option	Description
Re-configure Intel AMT	When this option is selected, the Intel SCS will apply all the current settings in the profile associated with each Intel AMT device according to the defined interval. Default: 11 months
Change Intel AMT Administrator password	The administrative user has access to all functions of the Intel AMT device. Only the Intel SCS has access to this ACL entry. When this option is selected, the administrative password is changed periodically to either a randomly-generated password or to a fixed password. The option used is defined in the profile that is associated with each Intel AMT device, on the General tab. See "Setup and configuration profile: General tab" on page 27. Normally, this maintenance function is used only with the random password option. Default: 1 month
Synchronize Intel AMT Clock	This option synchronizes the clock in each Intel AMT device to the clock on the Intel SCS platform. This operation is critical when using Kerberos authentication. It ensures that the clocks do not differ by more than the Kerberos Max Clock Tolerance defined in the Profiles. See "Setup and configuration profile: General tab" on page 27.

Security keys page

Setup and configuration of Intel AMT 2.0 (or later) devices is done using the TLS-PSK (Pre-Shared Key) protocol. The protocol requires the security keys installed both in the Intel AMT device and in the Intel SCS database. You can use the Security Keys page to manage the pre-shared keys and associated parameters. Each key has four elements: the key itself (PPS), an identifier sent in the clear by the Intel AMT device in the Hello message (called a PID), an initial MEBx password, and a replacement MEBx password.

Sets of these parameters can be generated, exported to a USB key, and then installed in new Intel AMT devices.

For more information, see the *Out of Band Management Component Implementation Guide*.

Alternatively, an OEM may ship initialized platforms with PID-PPS pairs and a default password already installed. In this case, you must import the key file from the OEM into Out of Band Management Component.

For more information, see the *Out of Band Management Component Implementation Guide*.

The third option is to generate new PID-PPS pairs, print them out, and type them into the Intel Management Engine (MEBx) manually.

For more information, see the *Out of Band Management Component Implementation Guide*.

If you are using the remote configuration feature of Intel AMT 3.0, the keys are generated and installed automatically.

For more information, see the *Out of Band Management Component Implementation Guide*.

Table 2-17 Options on the Security keys page

Option	Description
Add	Click to add a new security key. The PID is the 8 character identification string sent in the clear in the Hello message. The string format is "XXXX-XXXX". The PPS is a 32-character key string that is the secret shared between the Intel AMT device and the SCS service. The string format is "XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX". Type the factory default Intel Management Engine (MEBx) password. The default value is "admin", unless you specifically asked the OEM to pre-configure Intel AMT computers with a different password. Type a new password. This will become the new Intel Management Engine (MEBx) password after you initialize the Intel AMT device with this PID-PPS pair. **Note:** You must type a strong password. Example: P@ssw0rd For more information, see the *Out of Band Management Component Implementation Guide*.

Table 2-17 Options on the Security keys page *(continued)*

Option	Description
Generate security keys	Type the number of security keys to generate. Type a number equal or greater than the number of Intel AMT computers you want to initialize with the USB key. Each key will be used only once. There is no problem with exporting extra keys for use later or even not at all. Type the factory default Intel Management Engine (MEBx) password. The default value is "admin", unless you specifically asked the OEM to pre-configure Intel AMT computers with a different password. Type a new password. This will become the new Intel Management Engine (MEBx) password after you initialize the Intel AMT device with this PID-PPS pair. **Note:** You must type a strong password. Example: P@ssw0rd For more information, see the *Out of Band Management Component Implementation Guide*.
Mark selected security keys as already used	Click to mark a set of security keys that you have used to initialize an Intel AMT device manually. All marked security keys will disappear from the Security Keys page so the keys cannot be reused. However, the keys and passwords stay in the Intel SCS database and are used for initialization of Intel AMT devices. Marking the keys is necessary if you use the MEBx initialization method. For more information, see the *Out of Band Management Component Implementation Guide*.
Print security keys	Click to print the security keys and use them to initialize Intel AMT computers manually through MEBx. For more information, see the *Out of Band Management Component Implementation Guide*.
Export security keys to USB key	Click to write the current list of keys to a file on a USB Key. Click Generate. A file will be generated in the format expected by the platform BIOS. Click the Download USB key file link. Save the file to a FAT16-formatted USB key. Use the USB key to manually initialize the Intel AMT computers. For more information, see the *Out of Band Management Component Implementation Guide*.

Table 2-17 Options on the Security keys page *(continued)*

Option	Description
Import security keys	Click to import a file of keys, which you have received from an OEM together with initialized Intel AMT capable computers, into the Intel SCS database. Browse to the file and click Import. For more information, see the *Out of Band Management Component Implementation Guide*.

Service location page

This page lets you specify the location of the Intel Setup and Configuration Service (Intel SCS). By default, the Intel SCS is installed on the Notification Server computer, as part of the main OOB site server.

For more information, see the *Out of Band Management Component Implementation Guide*.

If you move the OOB site server to another computer, you must set the service URL to that of the new OOB site server.

Table 2-18 Options on the Service Location page

Option	Description
Default URL	By default, Out of Band Management Component looks for Intel SCS on the Notification Server computer.
Alternative URL	Displays the URL of the Intel SCS, installed on the OOB site server. To fill in this field automatically, in the Site Servers section, select a site server and click the Set as default location of Intel SCS symbol.
Site Servers	Lists the OOB site servers known to Out of Band Management Component.
System Status	Displays computers that have Intel SCS installed and their status.

Users page

The Users list defines identities with access to the Intel SCS configuration pages in Out of Band Management Component. Each user is assigned a role which defines the permissions that are allotted to the user. When Microsoft Active Directory is integrated with the Intel SCS and Intel AMT, you can import user identities from Active Directory. Otherwise, you can add user identities manually.

When you install Out of Band Management Component for the first time, all users in the Altiris Administrators group automatically become Intel SCS Enterprise Administrators with access to all Intel SCS features. If you want another user to access the Intel SCS interface, you must add that user to this list manually.

For more information, see the *Out of Band Management Component Implementation Guide*.

Table 2-19 Options on the Users page

Option	Description
Add	Click to add a user. Type or browse to a user name. From the Role drop-down list, select a role: ■ Enterprise Administrator - The Enterprise Administrator has access to all Intel SCS configuration and management screens, fields, and parameters. ■ Administrator - The Administrator role has the same permissions as the Enterprise Administer but does not have permission to create or edit Profiles, or access to the Users, General Configuration, or Maintenance functions. ■ Operator - The Operator role has access to the following: can view the Security Keys page; can view the Intel AMT Systems page; can view the standard log and the security audit log; can access the complete configuration parameters branch. ■ Log Viewer - This role allows a user to view the standard log and the security audit log.
Edit	Click to edit the user.
Delete	Click to delete the user. **Warning:** Never remove the user that is used by the SCS service when it is started. Removing this user causes the service to fail.

Delayed Setup and Configuration page

Note: This policy applies to Intel AMT releases 2.2, 2.6, 3.0, 4.0, and 5.0.

The Delayed Setup and Configuration policy lets you resume sending setup and configuration requests by initialized Intel AMT devices, which has stopped doing so because of timeout. This policy is also used to initiate the Remote Configuration sequence on Intel AMT 2.2 and 2.6 devices.

Delayed Setup and Configuration is an in-band functionality and requires a Windows operating system running and task agents installed on the client computer.

Computers that entered the delayed configuration state appear in the All Intel AMT Computers in Delayed Configuration State filter.

For more information, see the *Out of Band Management Component Implementation Guide*.

Table 2-20 Options on the Delayed Setup and Configuration page

Option	Description
DNS suffix	(Optional) You can type the DNS suffix that Out of Band Task Agent will configure the Intel AMT device with.
Override OTP	If you want to override the random one-time password that is sent to the Intel AMT device for authentication, check Override OTP and type a strong password. For more information, see the *Out of Band Management Component Implementation Guide*.
Switch to AMT	Check if you want the Out of Band Task Agent to enable Intel AMT in the client computer's BIOS. **Note:** The computers, that have "ASF" or "None" selected in the MEBx, will not appear in the default All Intel AMT Computers in Delayed Configuration State filter. If you want to switch such computers to Intel AMT, assign this policy to a custom filter. Example: All Intel AMT Capable Computers.
Ignore intermediate errors	If you want the Delayed Setup and Configuration process to continue even if some errors occurred, check Ignore intermediate errors. Set the scheduling options.

Intel AMT systems page

This page lets you view the list of the Intel AMT devices that have sent Hello messages to Intel SCS. These devices can be in a configured or unconfigured state. You can update the configuration of one or all of the already configured devices, among other operations.

Table 2-21 Options on the Intel AMT systems page

Option	Description
Authorize systems	This operation authorizes configuration for the selected devices. This operation becomes available when you check Intel AMT requires authorization before configuration on the General page. See "General page " on page 37. If you have computers in delayed configuration state and checked One time password required on the General page, then a one-time password is required for authorizing computers. Normally, the Intel SCS knows the one-time password it has set on the Intel AMT device at the time the Delayed Configuration policy has run, but you can also check Override OTP and specify a password manually. See "Delayed Setup and Configuration page" on page 44.
Update ACL	This operation updates the list of Intel AMT users, according to the ACL entries in the profile that is associated with each device and their access privileges. See "Setup and configuration profile: ACL tab" on page 32.
Renew RNG key	This operation resets the random number generator key for selected devices.
Update power policy	This operation updates the power policy for all devices according to the parameters that are defined in the profiles. See "Setup and configuration profile: Power policy tab" on page 35.
Synchronize clock	This operation synchronizes the clocks between the Intel AMT devices and Intel SCS.
Change connection state	Changes the computer's connection state from "connected" or "unconnected".
Assign profile	This operation lets you assign an FQDN and a configuration profile to the selected unconfigured Intel AMT device. The device will become configured using the supplied FQDN and profile next time the Hello message is sent. For more information, see the *Out of Band Management Component Implementation Guide*.

Table 2-21 Options on the Intel AMT systems page *(continued)*

Option	Description
Create assignments	This operation lets you assign profiles to multiple unconfigured Intel AMT computers. For more information, see the *Out of Band Management Component Implementation Guide*.
Re-configure	This operation applies all the current settings in the profile that is associated with each Intel AMT device.
Unconfigure	This operation disables each Intel AMT device and leaves it without any Setup and Configuration parameters. Unconfiguration is possible in the following ways: ■ Full: Deletes all data from each Intel AMT device. The Intel AMT devices are not functional. You have to initialize the device again. For more information, see the *Out of Band Management Component Implementation Guide*. ■ Partial: Deletes all data on every Intel AMT device except for the PID, PPS, and Administrator password. The devices will immediately start sending Hello messages. The SCS will set up and configure the devices according to the profiles that are associated with them. **Note:** When you unconfigure a notebook computer with Intel AMT, the wireless connection is lost. To configure the computer, connect it to the wired network.
Export the list of the systems	This operation backs up the current UUID to FQDN and profile mapping. The exported .CSV file can later be imported into the Profile Assignments page.
Open log for this system	Lists Intel SCS log entries that are filtered by the system's UUID.
Show detailed system information	Displays configuration information for the selected system.
Delete	Deletes the selected devices and the associated log entries from the Intel SCS database. For example, you can delete non-existing devices. Also, you will have to delete the device if it was unconfigured manually through the Intel Management Engine (MEBx).

Profile assignments page

An initialized Intel AMT device (with the PID-PPS pair installed) starts sending Hello messages and requesting configuration information from Intel SCS. A part of the Hello message is the Universal Unique Identifier (UUID) of the device. The Intel AMT device can be configured only when it has a configuration profile that is assigned to that UUID. You can create the profile assignments manually or automatically by the Resource Synchronization policy.

For more information, see the *Out of Band Management Component Implementation Guide*.

On the Profile Assignments page you can monitor and modify profile assignments.

Table 2-22 Options on the Profile assignments page

Option	Description
Add	Lets you add a new UUID to FQDN mapping. The device will become configured using the supplied FQDN and profile next time the Hello message is sent. For more information, see the *Out of Band Management Component Implementation Guide*.
Edit	Lets you edit a profile assignment.
Export the systems mapping	Backs up the current profile assignments.
Import system mappings	Imports profile assignments.
Delete	Deletes assignments.

Resource Synchronization page

This page lets you configure automatic configuration profile assignment to new Intel AMT devices that request configuration from Intel SCS.

This page also lets you configure a schedule, on which the configuration profiles are re-assigned, the Intel SCS and the Notification Server resources are synchronized, and duplicates are removed.

For more information, see the *Out of Band Management Component Implementation Guide*.

Table 2-23 Options on the Resource Synchronization page

Option	Description
Override existing profile assignments	Check to assign the profile defined on this page to the Intel AMT computers that already have a configuration profile assigned. This option changes the profile assignment, but does not re-configure the Intel AMT device with the new configuration profile.
Re-configure Intel AMT if assignment changes	Check to reconfigure the Intel AMT computers whose configuration profile assignments has changed. This option re-configures the Intel AMT device with the new configuration profile.
Add	Click to add a profile assignment. You can create a different profile assignment for each domain.
Use DNS IP resolution to find FQDN when assigning profiles	Check if you want to assign an FQDN to an Intel AMT computer that does not have the Altiris Agent installed and whose FQDN is not known to the Notification Server.
Remove duplicate Intel AMT resources from Notification Server database	Check to delete duplicate resources when synchronizing the Intel SCS and the Notification Server resources.
Add schedule	Add a schedule on which the policy will run.
Last synchronization statistics	Shows the last run statistics: the number of Intel AMT devices with profiles assigned, Notification Server computer resources created, and duplicate Notification Server computer resources cleaned.

Resource Synchronization: Assign profile dialog box

You can configure the Resource Synchronization policy to assign different profiles to computers from different domains. This dialog box lets you add a domain-to-profile mapping.

Table 2-24 Options on the Assign profile dialog box

Option	Description
Domain	Type the domain for which you want to create the mapping. You can also type a domain suffix. In this case, the Resource Synchronization policy assigns the profile you specify here to the computers from subdomains. For example, if you type `mydomain.com`, the computers from `subdomain.mydomain.com` also get the profile you specify here.
AD OU	If you enabled Active Directory integration, select the organizational unit where you want to register the AMT objects. See "Integrating Intel SCS with Active Directory" on page 59. Example: IntelAMT
Profile	Select the configuration profile you want to assign automatically to all new Intel AMT devices from the domain you specified here.

Get ASF/DASH Configuration Inventory task

This task lets you get the ASF or DASH settings (inventory) from client computers. The ASF/DASH inventory is collected and sent to the Notification Server in the standard Notification Server Inventory format.

Note: The Out of Band Task Agent must be installed on the client computers before running the task. The client computer must be turned on to run this task. The operating system must be running.

For more information, see the *Out of Band Management Component Implementation Guide*.

To get ASF or DASH inventory, run this task one time or on a schedule.

For information on running tasks, see the *Symantec Management Platform Help*.

Update ASF Configuration Settings task

The Update ASF Settings task lets you enable ASF and configure ASF settings remotely on client computers.

Note: The Out of Band Task Agent must be installed on the client computers before running the task. The client computer must be turned on to run this task. The operating system must be running.

For more information, see the *Out of Band Management Component Implementation Guide*.

Table 2-25 Options on the Update ASF Configuration Settings task

Option	Description
Modify ASF general settings	Check to modify the settings in this group when the task runs.
Enable ASF	Check to enable ASF.
Management console IP	Type the IP of the management console. Example: Type the Notification Server's IP.
SNMP community	Type the SNMP community name. This string acts as a password. Example: public
Transmit system heartbeat messages	Check to have the network adapter transmit periodic system heartbeat or entity presence messages to the management console and indicate the managed client computer is still operating.
Modify security settings	Check to modify the settings in this group when the task runs.
Generation key Operator authentication key Administrator authentication key	The scope of these keys (shared by multiple managed client computers and the management console or pair-wise unique for each managed client computer and the management console) is a local policy issue that is determined by the equipment owner at the time of installation.
Random number seed	If you want to update the random number seed, type the new seed.
Modify Intel ASF adapter settings	Check to modify the settings in this group when the task runs. The settings in this group will be applied to the computers with Intel ASF only.

Table 2-25 Options on the Update ASF Configuration Settings task *(continued)*

Option	Description
Timers	Check to modify the settings in this group when the task runs.
Enable OS hang watchdog	Check to watch for operating system hangs and type the watch interval in seconds. Default: 30 seconds.
Enable ping to management console	If you want the network adapter to ping the management console, check this option and type the ping interval in seconds. If the ping fails, the agent goes into safe mode. Default: 30 seconds.
Spanning tree	Check to modify the settings in this group when the task runs.
Ping destination on link reconnect	If you want the network adapter to ping the management console after the link is temporarily lost and then restored, check this option and type the interval in seconds and the count of pings. Default: 10 seconds, 3 times.
Delay sending Platform Event Traps on link reconnect	If you want to delay sending events to the management console after the link is restored, for example if the network traffic is high, check this option and type the number of seconds to wait. Default: 10 seconds.
Remote control settings	Check to modify the settings in this group when the task runs.
ASF Reset	Check to enable a low latency reset of the system.
ASF Power Down	Check to enable unconditional power-down (occurs without any blocking from software or system).
ASF Power Up	Check to ensure that the sleeping system can be remotely turned on.
ASF Power Cycle	Check to enable a hard reset of the system. This reset is functionally equivalent to an unconditional power-down operation, followed by a power up.
Modify Broadcom ASF adapter settings	Check to modify the settings in this group when the task runs. The settings in this group will be applied to the computers with Broadcom ASF only.

Table 2-25 Options on the Update ASF Configuration Settings task *(continued)*

Option	Description
Wake on ARP or RMCP traffic	Check to configure the network adapter to wake the computer upon receiving ARP or RMCP traffic while the computer is in low-powered mode.
Enable remote management	Check to enable the receipt and handling of Remote Management Control Protocol (RMCP) messages by the network adapter.
Events settings	Check to modify the settings in this group when the task runs.
Enable platform event Trap (PET) messages	If you want the network adapter to transmit PET messages, check this option.
PET retransmission interval	Specify the time interval (in seconds) between retransmission of a PET message. Default: 20 seconds.
Modify system management bus settings	Check to modify the settings in this group when the task runs.
Legacy poll interval	Type the minimum time to wait for the ASF sensor inter poll. Default: 15 seconds.
Legacy poll delay	Type a delay in seconds. Default: 15 seconds.
Security	Check to modify the settings in this group when the task runs.
Use security management (ASF 2.0)	Check to enable a set of security extensions that provide authentication and integrity services for Remote Management Control Protocol (RMCP) messages introduced by ASF 2.0.
Use ASF 1.0 compatibility	Check to turn on ASF 1.0 backward compatibility support.
Session timeout	In this box, specify the timeout for authentication during session setup. Default: 300 seconds.
Remote control settings	Check to modify the settings in this group when the task runs. You can enable Operator, or Administrator rights, or both.
ASF Reset	Check to enable a low latency reset of the system.

Table 2-25 Options on the Update ASF Configuration Settings task *(continued)*

Option	Description
ASF Power Down	Check to enable unconditional power-down (occurs without any blocking from software or system).
ASF Power Up	Check to ensure that the sleeping system can be remotely turned on.
ASF Power Cycle	Check to enable a hard reset of the system. This reset is functionally equivalent to an unconditional power-down operation, followed by a power up.

Update DASH Configuration Settings task

The Update DASH Configuration Settings task lets you enable DASH and configure DASH settings remotely on client computers.

Note: The Out of Band Task Agent must be installed on the client computers before running the task. The client computer must be turned on to run this task. The operating system must be running.

For more information, see the *Out of Band Management Component Implementation Guide*.

Table 2-26 Options on the Update DASH Configuration Settings task

Option	Description
Enable DASH	Check to enable DASH.
Modify security settings	Check to modify the settings in this group when the task runs.
RMCP Ping Only	Check to disable all management functionality except for sending out a presence ping, which lets the management console discover DASH capabilities of the client computers.
Modify Web Services-based settings	Check to modify the settings in this group when the task runs.
HTTP Session Timeout	Set the management session timeout value. Default: 30 seconds.

Table 2-26 Options on the Update DASH Configuration Settings task *(continued)*

Option	Description
HTTP GET (HTML User Interface)	Check to allow only HTTP GET requests.
HTTP Digest Authentication only	Check to allow connection using Digest authentication only.
HTTP Support	Check to allow DASH management through HTTP.
Secure HTTP Support	Check to allow DASH management through HTTPS.
PKCS#1 DER-encoded 1024-bit RSA Key	Check to replace the security key on the DASH device. Browse to the key in the expected format.
TLS/SSL Server DER-encoded X.509 Certificate	Check to replace the certificate on the DASH device. Browse to the certificate in the expected format.
Modify Administrator account password	Check to modify the settings in this group when the task runs.
Password	Type the new password for Administrator account.

OOB Site Service page

On this page, configure the OOB Site Service installation settings.

For more information about the OOB Site Service, see the *Out of Band Management Component Implementation Guide*.

The settings you configure on this page take effect at the time of OOB site server installation. After you installed an OOB site server, you can use the General page to configure the settings.

See "General page " on page 37.

Table 2-27 Options on the OOB Site Service page

Option	Description
SQL settings	Type the SQL server's hostname and the database name Intel SCS will work with. Default database name for 7.x release of Out of Band Management Component is Symantec_CMDB_IntelAMT. If you upgraded from version 6.x of Out of Band Management Component and want to reuse old database, type the name of the database you used in 6.x (IntelAMT).

Table 2-27 Options on the OOB Site Service page *(continued)*

Option	Description
SQL Access	Select Use Windows authentication (default) for Intel SCS to connect to the SQL server using the Notification Server's application identity. If you want to use SQL authentication, select Use SQL Server authentication and specify the user ID and password.
Re-use database if exists	When selected, Intel SCS installation re-uses the existing database with Intel AMT data in it. By default, this check box is selected. Clear this check box only if you want to clear the database on Intel SCS install. **Caution:** All OOB site servers in your environment use the same database. Clearing this check box when installing an OOB site server will remove all data about Intel AMT computers in your environment.
Remove database on uninstall	When selected, OOB site server uninstallation removes Intel SCS database. By default, this check box is cleared. Select this check box only if this is the last OOB site server in your environment and you want to remove the database. **Caution:** All OOB site servers in your environment use the same database. Removing the database when uninstalling will leave other OOB site servers unoperational.
AD Integration	When selected, the OOB site server installation will check if the site server candidate is part of the domain and can contact the Active Directory.
Use TLS for secured communication	When selected, the OOB site server installation will check if the Certificate Authority is accessible and the site server can support TLS.
Mutual TLS authentication	When selected, the OOB site server installation will check if the site server can support TLS mutual authentication.
802.1x connections	When selected, the OOB site server installation will check if the site server can support 802.1x connections.

Table 2-27 Options on the OOB Site Service page *(continued)*

Option	Description
Application Identity	Specify credentials to use when installing OOB Site Service to a site server. Selecting Use application credentials (default) installs OOB Site Service using the Notification Server's application identity credentials. If you want to install using other credentials, select Use these credentials and type the user name and password.
Listen Port	Each instance of Intel SCS listens for Hello messages from Intel AMT devices on a defined TCP port. Type the TCP port used for listening. The default port is 9971.
Active Directory integration	Selecting Schema Extension or Standard will cause the Intel SCS server to add AMT objects to Active Directory. This enables the use of Kerberos authentication and the Active Directory users list. Active Directory is also required for TLS Mutual Authentication and 802.1X profiles. Before you select AD integration, you must integrate Intel SCS with Active Directory. For more information, see the *Out of Band Management Component Implementation Guide*. See "Integrating Intel SCS with Active Directory" on page 59.
Allow Remote Configuration	Intel AMT releases 2.2, 2.6, 3.0, 4.0, and 5.0 support Remote Configuration. As part of this feature, the Intel AMT device sends a self-signed certificate for the TLS Mutual Authentication process. This certificate is used for setup and configuration only. The device creates the self-signed certificate just before sending the first "Hello" message. Selecting this check box enables the Intel SCS to accept self-signed certificates from Intel AMT devices. For more information, see the *Out of Band Management Component Implementation Guide*.
Use one time password	Selecting this check box adds an additional security feature. This will require a one-time password (OTP) exchange between Intel SCS and the Intel AMT device requesting setup and configuration.

Table 2-27 Options on the OOB Site Service page *(continued)*

Option	Description
First Common Name (CN) in certificate subject name	Select an option that matches your root certification authority certificate's CN field.
Log Level	The system wide actions log can be recorded at several levels. The more detail recorded, the more system resources and bandwidth must be allocated.

Viewing Intel SCS logs

Intel SCS is a service that is installed by Out of Band Management Component. Intel SCS handles the interaction with Intel AMT devices and creates logs to record these interactions. The logs are located in the Intel SCS database (Default: Symantec_CMDB_IntelAMT). If you have problems configuring, connecting to, managing, or otherwise interacting with the Intel AMT devices, you can check the logs through the Symantec Management Console.

If you want to view more detailed information in the logs, on the General page, change the log level.

To change the log level

1. In the Symantec Management Console, on the Home menu, click **Remote Management > Out of Band Management**.
2. In the left pane, click **Configuration > Configuration Service Settings > General**.
3. Under Log Options, in the Log level drop-down list, select the log level you want.

   For example, select Detailed verbose to see the most detailed information in the logs.

To view Intel SCS logs

1. In the Symantec Management Console, on the Home menu, click **Remote Management > Out of Band Management**.
2. In the left pane, click **Configuration > Logs**.
3. View the logs.

   The log choices are:

Action Status	These records provide general maintenance, success, and error messages that are related to the functions of Intel SCS. These logs show general configuration, communication, and Active Directory integration messages. This log displays asynchronous actions, such as global operations or operations per Intel AMT device, that are entered into the queue. Their status in the queue is also displayed. The Name field shows the attempted action. The Status field shows success or failure or whether an action is queued, delayed, or in progress.
Logs	These records provide the information that is related to Notification Server interactions with Intel AMT. These show information and errors from the Intel SCS (AMTConfig) service, including interaction with the IntelAMT database. These logs show the status on tasks such as RNG keys, configuration steps, hello packet errors and messages, and service status.
Security Audit	This log displays potential breaches in security, such as unauthorized attempts to log-in and unauthorized attempts to perform the re-configuration function on all Intel AMT devices.

   For more information, see the *Out of Band Management Component Implementation Guide*.

Integrating Intel SCS with Active Directory

(Intel AMT only)

Microsoft's Active Directory (AD) is a directory service that integrates with Windows 2003 Server. AD is an optional environment pre-requisite.

You must integrate Intel SCS with AD if you want to use the following Intel AMT features:

- Kerberos authentication using AMT objects
- User lists

- TLS Mutual Authentication
- 802.1X Profiles

To integrate Intel SCS with Active Directory

1. Ensure the OOB site server computer (by default, the Notification Server computer) is registered in a domain.
2. Create a new Organizational Unit in the Active Directory for Intel AMT devices as follows:
   - On the domain controller computer, in the Administrative Tools, click **Active Directory Users and Computers**.
   - Right-click on the domain node, and then click **New > Organizational Unit**.
   - Type the name of the unit.
     Example: IntelAMT

     Warning: Do not use spaces in the organizational unit's name.

   - Click **OK**.

   Later, when you assign configuration profiles to Intel AMT devices, you can specify the Organizational Unit where the configured Intel AMT devices are registered.
3. In the Symantec Management Console, on the Home menu, click **Remote Management > Out of Band Management**.
4. In the left pane, click **Configuration > Configuration Service Settings > General** .
5. In the Active Directory Integration drop-down list, click one of the following options:

Standard	Integrate with Active Directory without extending the schema.
Schema Extension	Integrate with Active Directory and cause the SCS server to add AMT objects to Active Directory. We recommend using this method.

6. If you selected Schema Extension, do the following steps:
   - Click the **Extend Active Directory schema** link.

- Type the credentials of a user who is a member of both the "Domain Admins" and "Schema Admins" groups.
- Click **Extend**.
- Click **Close**.

7 From the Default AD OU drop-down list, click the name of the Organizational Unit that you created.

In this example, click **IntelAMT**.

8 Click **Save changes**.

Glossary

ACL (Access Control List)	A list of permissions that is attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object. In a typical ACL, each entry in the list specifies a subject and an operation. In Intel AMT, ACL is a list of users and their access privileges.
AD (Active Directory)	An advanced, hierarchical directory service from Microsoft. It is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories. Active Directory is designed especially for distributed networking environments.
agent presence	A security toolset that is built into Intel AMT. This toolset enables management applications to configure Intel AMT devices to monitor for the presence of software agents, such as antivirus and firewall applications that run on the Intel AMT system platform. The management application configures the Intel AMT device with timers set to detect when the software agent initializes and periodically transmits presence signals. Using this toolset, IT technicians can identify computers with disabled or uninstalled software agents and take appropriate actions.
Altiris 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 Altiris Agent also lets you install and manage solution plug-ins that add functionality to the agent.
ASF (Alert Standard Format)	An industry standard-based technology that lets IT administrators manage computers regardless of the operating system state. ASF provides alerts and power management functionality as long as the computer is plugged in with an Ethernet connection. ASF functions through hardware on the network card or system board, a software agent on the client computer, and management software on the server.
Circuit Breaker	A security toolset of Intel AMT. This toolset represents a set of hardware-based network packet filters. IT technicians can apply these filters to computers that send suspicious network packets to seal infected computers from the rest of the network.
CMDB (Configuration Management Database)	The central database that stores all information about the Symantec Management Platform and its managed computers.

DASH (Desktop and Mobile Architecture for System Hardware)	A Web services-based management technology that lets IT professionals remotely manage desktop and mobile computers. Administrators can securely turn on or off the power, query system inventory, and push firmware updates regardless of the state of the remote computer.
discovery	The process of searching for computers or other resources on your network that meet specific requirements.
DNS (Domain Name System)	A system that converts host names and domain names into IP addresses on the Internet or on the local networks that use the TCP/IP protocol. For example, when a Web site address is given to DNS, DNS servers return the IP address of the server that is associated with that name.
event	Any action that Notification Server can monitor.
filter	A query that identifies a dynamic group of resources that share common criteria.
FQDN (fully qualified domain name)	The complete domain name for a specific computer, or host, on the Internet. The FQDN consists of two parts: the host name and the domain name. An example is mycomputer.mydomain.com.
IDE-R (IDE-Redirection)	An Intel AMT built-in hardware capability. It lets IT administrators start a computer from an image that is stored on the network or on the remotely mounted CD-ROM or hard drive.
in-band management	A type of remote computer management. It requires the target computer's operating system to be initialized and to function properly.
Intel AMT (Intel Active Management Technology)	A solution that is based in hardware and firmware and is connected to the system's auxiliary power plane. Despite the power state or the operating system state of the client computer, Intel AMT provides IT administrators with access to alerts, hardware inventory, power management, circuit breaker, and agent presence functionality. Intel AMT functionality requires the computer to be plugged into the power source and connected to the network. Intel AMT functionality does not require a software agent to be installed on the client computer.
Intel SCS (Intel Setup and Configuration Service)	A software that provides the tools to set up and configure Intel AMT-capable computers for out-of-band management. Out of Band Management Component integrates Intel SCS into the Notification Server infrastructure and provides the interface for Intel SCS in the Symantec Management Console.
Kerberos	A system that provides authenticated access for users and services on a network.
key	A piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of plain text into ciphertext or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and keyed-hash functions (also known as MACs), often used for authentication.
managed computer	A computer on which the Altiris Agent is installed.

MEBx (Intel Management Engine BIOS extension)	A BIOS extension that is used to manually configure the Intel AMT device that is installed on a computer.
mutual authentication	A process where two parties, typically a client and a server, authenticate each other. This authentication lets both parties know of each other's identity. In mutual authentication, the server also requests a certificate from the client. Also called two-way authentication.
Notification Server	The Symantec Management Platform service that communicates with the Altiris Agent and the CMDB to provide management, security, and administrative functionality. It processes events, facilitates communications with managed computers, and coordinates the work of the other Symantec Management Platform services.
out-of-band management	A type of remote computer management. It lets IT administrators connect to a computer's management controller when the computer is turned off, in sleep or hibernate modes, or otherwise unresponsive through the operating system. Out-of-band management can be performed on the computers that have Intel AMT, DASH, or ASF-capable network adapters.
permissions	The rights that a user or group has to access different items within the Symantec Management Console. Permissions are granted to users through their security role.
PET (Platform Event Trap)	An event that is originated directly from platform firmware (BIOS) or platform hardware (ASIC, chipset , or microcontroller) independently of the state of the operating system or system management hardware. PET events provide advance warning of possible system failures.
policy	A set of rules that control the execution of automated actions. Policies can be scheduled or based on incoming data that triggers an immediate action. Policies determine when an action should start and who or what should be notified of the results.
power state	The overall power consumption of the system. Six power states exist that range from S0 (the system is powered on and fully operational) to S5 (the system is powered off). States S1, S2, S3, and S4 are referred to as sleeping states.
PSK (Pre-Shared Key)	A shared secret that was previously shared between the two parties using some secure channel before it needs to be used.
PXE Boot (Pre-Boot Execution Environment)	An environment to start computers using a network interface independently of available data storage devices (like hard disks) or installed operating systems. An administrator can load operating systems and other software onto the device from a server over the network.
resource	Any item that Notification Server can track or manage, such as a user, site, installed application, computer, switch, router, or handheld device.

Resource Manager	A feature that displays information about a resource, such as its properties and current state. It also lets you troubleshoot and perform actions on managed resources.
site server	A managed computer on which a service plug-in is installed. Notification Server can reduce its workload and minimize network traffic by distributing specific processes to site servers.
SOL (Serial-over-LAN)	A feature of Intel AMT that redirects console output to a remote terminal. It lets IT administrators remotely change BIOS settings, repair a computer that cannot start, and so on.
SOL/IDE-R (Serial-over-LAN/IDE-Redirection)	The proprietary protocols that are defined for Intel AMT that redirect keyboard, text, floppy disk, and CD transfers from a local host to a remote workstation.
Symantec Management Console	The Web-based user interface for managing 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 services.
task	An action that is performed on a computer. Server tasks are run on Notification Server. Client tasks are run on managed computers.
TLS (Transport Layer Security)	A protocol that is intended to secure and authenticate communications across a public network through data encryption.
VLAN (Virtual LAN)	A logical subgroup within a local area network that is created through software rather than by manually moving cables in the wiring closet. It combines user stations and network devices into a single unit regardless of the physical LAN segment they are attached to. It also lets traffic flow more efficiently within populations of mutual interest.

Index