

# Intel® Active Management Technology Setup and Configuration Service Version 5.0

## *Console User's Guide*

Document Release Date: July 9, 2008



Information in this document is provided in connection with Intel products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

The API and software may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

This document and the software described in it are furnished under license and may only be used or copied in accordance with the terms of the license. This document may be reproduced, in whole or in part, solely for the purpose of end user documentation in support of products that use the Setup and Configuration Server or its components, so long as proper attribution is provided to Intel and all proprietary marks are preserved. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document. Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an ordering number and are referenced in this document or other Intel literature may be obtained by calling 1-800-548-4725 or by visiting Intel's web site at <http://www.intel.com>.

Copyright © 2006, 2007, 2008 Intel Corporation

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

\* Third party other names and brands may be claimed as the property of others.

# Part I

---

## Introduction

This part contains the following chapters:

- Overview of the Intel SCS Console



---

# Table of Contents

**PART I: INTRODUCTION**

**Chapter 1: Overview of the Intel SCS Console ..... 5**

About This Book ..... 5

Introduction to Intel SCS ..... 6

Intel SCS Components ..... 7

Setup and Configuration Steps ..... 8

Before Setup and Configuration ..... 9

Intel AMT SCS Functional Flow ..... 10

Setup and Configuration Operational Overview ..... 12

**PART II: QUICK START**

**Chapter 2: SCS Console Flow ..... 19**

Specify Platform Configuration Parameters ..... 19

Add SCS Users ..... 19

Create Profiles ..... 19

Specify Console Settings ..... 20

Create USB Key with TLS-PSK Keys (if required) ..... 20

Configure Global Settings (if required) ..... 20

**Chapter 3: Connecting to the SCS ..... 21**

Logging On ..... 21

## PART III: CONSOLE OPERATIONS

<b>Chapter 4: Creating and Changing Profiles .....</b>	<b>27</b>
About Creating Profiles .....	28
Creating a Profile .....	29
Changing Network, Security or Power Management Settings .....	31
Configuring ACL Settings .....	35
Specifying Domains .....	41
Configuring TLS Settings .....	44
Configuring 802.1x .....	47
Configuring WiFi .....	55
Configuring CIRA (Client-Initiated Remote Access) .....	57
Viewing and Editing a Profile's Properties .....	63
<b>Chapter 5: Preparing and Managing Platforms .....</b>	<b>65</b>
Adding Device Configuration Information to SCS .....	66
Searching for Platforms .....	67
Adding a Platform Definition .....	67
Deleting Platform Information and/or Configuration Properties .....	69
Viewing and Changing Platform Settings .....	69
Creating and Viewing Collections .....	75
Deleting Collections .....	78
Exporting Lists of Machines .....	78
<b>Chapter 6: Console Settings .....</b>	<b>79</b>
Specifying Console Settings .....	79
<b>Chapter 7: Applying Operations to AMT Machines .....</b>	<b>81</b>
Reapplying Configurations .....	82
Resetting Configurations .....	84
Resetting a Platform or Collection to Factory Default Values .....	85
Updating ACLs .....	85
Setting CRLs .....	86
Setting Power Policies .....	86
Synchronizing Clocks .....	87
Setting Connection Status .....	87
Authorizing Setup and Configuration .....	88
<b>Chapter 8: Managing SCS Users .....</b>	<b>89</b>
About Users and Groups .....	89
SCS User Roles .....	90
Viewing Existing Users .....	92
Adding SCS Users .....	93
Deleting SCS Users .....	94
Changing a User's SCS Role .....	94

<b>Chapter 9: Using USB Drives for TLS-PSK Keys .....</b>	<b>95</b>
About Using USB Drives for Setup and Configuration .....	95
Configuring Pre-Setup and Configuration Security Keys .....	96
Creating TLS-PSK Security Keys .....	97
Exporting TLS-PSK Keys to a USB Drive .....	98
Importing Keys .....	101
<b>Chapter 10: Viewing and Configuring SCS Services .....</b>	<b>103</b>
About SCS Service Settings .....	103
Network Settings .....	104
Maintenance Policies .....	106
Log Settings .....	108
AMT Configuration Parameters .....	109
Performance Settings .....	111
<b>Chapter 11: Viewing Log files .....</b>	<b>113</b>
About the Log Files .....	113
Using the Event Logs .....	114
Using the Operations Log .....	119
Creating View Collections .....	121
Creating View Subcollections .....	126
Exporting Log Files .....	127
<b>Chapter 12: Localization .....</b>	<b>129</b>
Internationalization of SCS Messages .....	129

## **PART IV: APPENDIXES**

<b>Appendix A: Remote Configuration .....</b>	<b>133</b>
About Remote Configuration .....	134
Remote Configuration Flow .....	135
Intel AMT Release 3.0 Additional Features .....	145
Remote Configuration Certificate – Differences between Releases .....	146
Intel® vPro™ Technology Activator Utility .....	147

<b>Appendix B: CRL XML Format .....</b>	<b>149</b>
---	------------

<b>Appendix C: Using a Script to Import Intel AMT Configuration Properties</b>	<b>153</b>
Environment Variables .....	153
Output File Format .....	154
Script Functionality .....	155
Sample Scripts .....	155





# 1

## Overview of the Intel SCS Console

This chapter provides a brief description of the Intel® AMT Setup and Configuration Service and lists its components. For detailed information about the application, refer to the *Intel® AMT Setup and Configuration Service User's Guide*.

This chapter contains the following sections:

- About This Book
- Introduction to Intel SCS
- Intel SCS Components
- Setup and Configuration Steps
- Before Setup and Configuration
- Intel AMT SCS Functional Flow
- Setup and Configuration Operational Overview

### About This Book

This book provides instructions on using the Intel® AMT Setup and Configuration Console.

## Introduction to Intel SCS

The Intel® Active Management Technology (Intel® AMT) Setup and Configuration Service (Intel SCS or SCS) provides an enterprise with the tools to set up and configure Intel AMT devices.

**Note:** In addition to the term “Setup and Configuration”, the process of enabling an Intel AMT device is sometimes referred to as “provisioning.”

The Intel AMT Setup and Configuration Service performs all the necessary steps to make an Intel AMT device operational. This includes Intel AMT Release 2.0 and later releases.

Once the Intel SCS has been installed and its database has been loaded with initial data, setup and configuration starts when an Intel AMT device sends a message called a “Hello” message to the SCS. The SCS and the Intel AMT device communicate securely as the SCS generates and sends the following information to the device:

- certificates from a public key infrastructure (PKI)
- access control lists (ACLs)
- other setup parameters, as defined in a **profile** of setup and configuration information specific to the platform or to a family of platforms

The SCS also registers the Intel AMT device in Active Directory and in its own secure database. The SCS is used for various maintenance functions, such as updating passwords and ACLs, and keeps logs of all performed transactions.

The SCS components can be distributed across several platforms. It is recommended, for performance reasons, to configure a distributed installation except when installing the SCS in small enterprises.

It is possible to have multiple instances of the SCS installed across an enterprise, but there is only one SCS database for the enterprise.

## Intel SCS Components

The Intel SCS includes several components.

The following are components of the Intel SCS.

### Main Service

This is the software component that processes Setup and Configuration Service requests from Intel AMT devices and is implemented as a Windows Service.

### SOAP API

This is the Application Programming Interface (API) that is used by the SCS Console to interact with the Main Service indirectly via the database server.

### Database Server

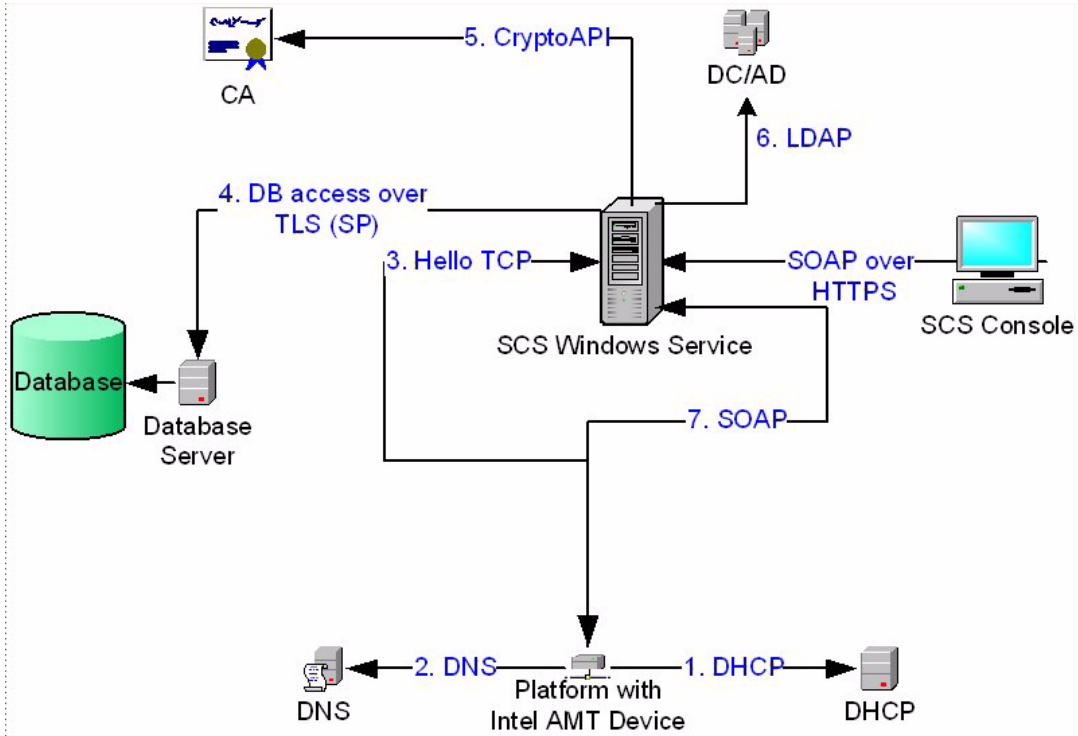
This is the secure repository that stores the Setup and Configuration data, organized according to the SCS database schema, and installed as a database instance in Microsoft SQL Server.

### Intel SCS Console

The Intel SCS Console is an application that is installed separately from the SCS. It is an open application that uses the SCS SOAP API to manage the SCS and the SCS database. The source is distributed with the SCS. An ISV can take the source, add value to it and integrate it into a Management Console product.

## Setup and Configuration Steps

The following diagram illustrates the major setup and configuration steps. The numbered steps are described below:



- 1** An Intel AMT device that is ready for setup requests an IP address from a DHCP server.
- 2** The device performs a DNS lookup with the default SCS service server name.
- 3** The Intel AMT device sends a TCP/IP “Hello” message.
- 4** Based on the UUID in the “Hello” message, the SCS service searches the database to locate the Profile and host name to be used to setup and configure the device. If the SCS is configured to do so, it may execute a script to acquire the necessary parameters from sources outside the database, and then store the information in the database.
- 5** The SCS service requests a certificate for the device from a Certification Authority server. This step is optional. It is required for installations using Transport Layer Security (TLS) and Mutual TLS.

- 6 The Intel AMT device is defined as an AMT object in the Active Directory domain controller, when integration with Active Directory is enabled.
- 7 The SCS service completes setup and configuration using SOAP commands. With Intel AMT Release 3.2 and later releases, the SCS performs setup and configuration using methods that create and communicate with WS-Management objects.

All critical parameters are kept in the secure database. The Administrator configures the SCS service, defines profiles, updates individual device parameters, and so on from the Intel SCS Console. The console communicates only with the SOAP API, which queries and updates the database. All instances of the SCS service poll the database periodically or query and update the database as needed as part of the setup and configuration process.

All of the above steps are described in this guide.

The Intel SCS includes several components. They can be installed on a single computer or on separate computers.

In addition, the environment must include several pre-installed and configured Microsoft components.

## Before Setup and Configuration

For setup and configuration to proceed, the SCS database and server require preparation, as well as the platform containing the Intel AMT device. Once the preparation is complete, connecting the platform to the network starts the setup and configuration process.

### SCS Database Preparation

Before setup and configuration can begin, the SCS server database must be configured with basic information:

- SCS service configuration parameters
- Profiles that define the setup parameters for the Intel AMT-enabled platforms to be configured
- Entries identifying each Intel AMT device to be configured, with a link to a profile. Note that it is also possible to get the configuration parameters from a script, when the AMT addresses the SCS.

- A list of valid TLS-PSK keys that match what is installed on the Intel AMT devices awaiting configuration.

At this point, the SCS service waits for a configuration request from an Intel AMT device.

## Preparation of Platform Containing Intel AMT Device

An Intel AMT Release 2.0/2.1/2.5 device must have its MEBx password changed from the default password. A TLS-PSK key and identifier must be loaded into the device. The values are entered manually by the IT administrator through the BIOS extension, or the administrator can use a USB key with values exported from the SCS; or the values may have been preloaded by an OEM. This is the minimum requirement, although other parameters may be required. See the AMT Setup Guide for more information. The platform can now be connected to a network in common with the SCS server.

An Intel AMT Release 2.2/2.6/3.0/4.0/5.0 device can be connected to the network without a password change or entry of any parameters to the BIOS extension, using a mechanism called “Remote Configuration”. For details of the remote configuration process, see Remote Configuration.

Intel AMT devices configured by the SCS receive their IP addresses from a DHCP server. The SCS does not support static IP addresses.

## Intel AMT SCS Functional Flow

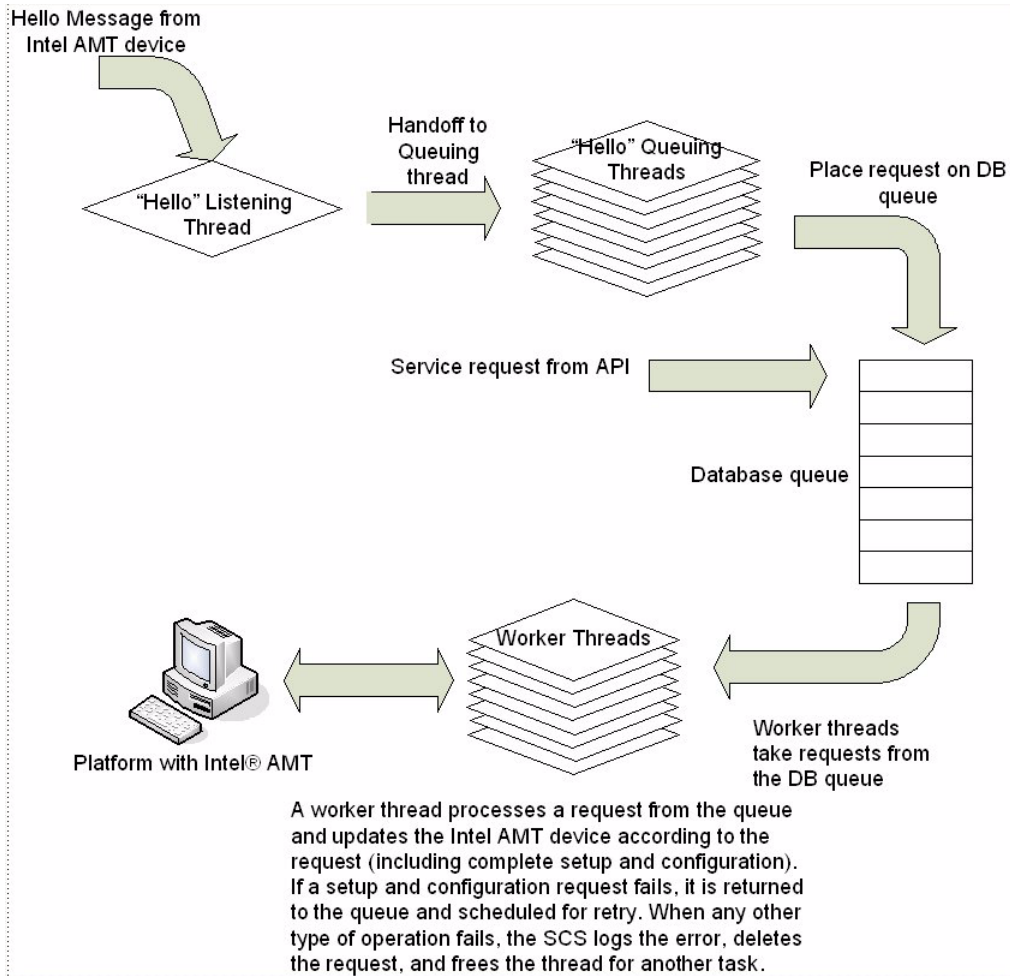
The SCS is designed to perform setup and configuration of multiple Intel AMT devices simultaneously. All requests to the SCS for service are maintained in a queue in the SCS database. A “thread” performs the processing for each portion of a task. A single thread waits for “Hello” messages from Intel AMT devices. This thread passes the message to a queuing thread, which then adds this request for setup and configuration to the database queue. Requests via the SOAP API to perform an update to an Intel AMT device are added to the queue directly by the API.

Worker threads in the SCS poll the queue for tasks. A worker thread will perform all steps required for setup and configuration. After a task completes, the SCS releases the thread for subsequent use by another task.

The SCS logs all transactions so that if the service is interrupted, the service can recover partially completed tasks.

IT administration can configure the number of worker threads, the queue size, and various times to maximize performance of the SCS. In an enterprise installation that has the potential of many Intel AMT devices requesting setup simultaneously, the number of worker threads can be increased, consistent with the number of processors and the amount of memory installed in the server platform. See Performance Settings for the tuning parameters accessible from the SCS Console.

The figure below presents a simplified flow within the SCS:



SCS Operational Flow

## Setup and Configuration Operational Overview

The primary purpose of the Intel SCS is to deliver the Intel AMT Setup and Configuration settings to the Intel AMT devices. Intel AMT devices can be located on, for example, a desktop computer, a mobile computer, or a workstation.

This process includes pre-setup and configuration; setup and configuration; integration with Active Directory, gathering security information, and maintenance.

### Pre-Setup and Configuration

Intel SCS generates data used to configure Intel AMT devices. This data includes:

- PPS, PID and MEBx password generation
- USB key file containing a list of PPS, PID and MEBx password sets

Remote configuration does not use these values.

### Setup and Configuration

Intel SCS delivers initial values to Intel AMT devices. Before Setup and configuration begins, administrators add these initial values to the database. The administrator enters the values into Profiles, or into descriptions of individual Intel AMT devices, or the information is generated automatically. The information includes:

- Administrator account credentials (Username and password)
- Access control list (ACL) entries for Digest and/or Kerberos user accounts
- Networking settings (Host Name and domain name)
- RSA key pair and X.509 certificate for TLS (TLS Certificate and RSA private key) (automatic)
- Pseudo Random Number Generator (PRNG) value
- Intel AMT Kerberos secret key (generated automatically), SPNs, operational parameters
- Time and date (automatic)
- Trusted root certificates (Mutual TLS)
- Trusted domain name suffixes (Mutual TLS)
- Certificate Revocation Lists (CRLs)



- Power-policy options
- Replacement PID/PPS
- Wireless Profiles
- 802.1x Profiles
- EAC Profiles

The information is used to communicate securely with an Intel AMT device to configure it and to create an Active Directory entry.

### Integration with Active Directory

Intel SCS integrates the Intel AMT device with Microsoft Active Directory by creating a directory entry based on the Intel-Management-Engine class. The SCS installation includes scripts used by the enterprise administrator to:

- Extend the Active Directory schema to support the Intel-Management-Engine class (optional). When not using the Intel-Management-Engine (with no schema extension) it uses the Computer class.
- Populate the Intel-Management-Engine attributes

During **setup**, Intel SCS:

- Creates an Active Directory object representing the Intel AMT device
- Creates an attribute for connecting the AD computer object to the AMT object.

### Gathering Security Information

Intel SCS collects required operational security parameters.

- As part of setting up the SCS, the administrator defines Active Directory users and permissions for those administrators and operators that will work with Intel SCS. The administrator uses scripts to define the necessary groups and users within Active Directory, and then uses the SCS User commands to define which users have specific permissions to operate the service.
- When TLS is enabled, the SCS interfaces with the Microsoft Certification Authority to obtain a TLS certificate each time it sets up an Intel AMT device.

## Management and Maintenance

Intel SCS also facilitates life cycle management and maintenance operations. These daily tasks can include:

- Entering the properties of new Intel AMT devices, such as the UUID, FQDN, profiles, and AD Organizational Unit (required for adding new Intel AMT-enabled platforms)
- Generating a dataset of PID/PPS/password data for export to a USB key
- Importing TLS-PSK lists from an OEM
- Handling certificate expirations and certificate renewals
- Delivery of Certificate Revocations Lists (CRL)
- Updating local account passwords
- Checking the logs
- Handling exceptions
- Doing ad-hoc configuration operations (Single Intel AMT device / All Intel AMT devices):
- Performing unconfiguring
- Performing reconfiguration
- Updating system clock
- Doing daily database backup

In addition to these tasks, certain maintenance tasks that enhance the security of the Intel AMT devices can be performed automatically. These include:

- Reissuing digital certificates before they expire
- Updating passwords
- Synchronizing the system clock
- Performing re-configuration periodically to ensure that all Intel AMT devices have the latest profile information

## Configuring Intel AMT to Work in a Secure Environment

Intel AMT supports Transport Layer Security (TLS) for secure communications between Intel AMT devices and management console applications. Use of TLS is recommended in an Enterprise environment. TLS is a protocol intended to secure and authenticate communications across a public network by using data encryption. It depends on the existence of a public key infrastructure (PKI).

A PKI enables users of an unsecured network to securely and privately exchange information through the use of an asymmetric public and private cryptographic key pair. The key pair is obtained and shared through a trusted authority, known as a Certification Authority (CA). The CA generates digital certificates that can identify an individual or an organization. The PKI includes directory services that can store and, when necessary, revoke the certificates.

If TLS will be used with Intel AMT devices, then there must be access to the Microsoft Certification Authority as the SCS requires it to enroll for certificates on behalf of each Intel AMT device.

The Microsoft CA can be installed as Stand-alone CA or as an Enterprise CA. An Enterprise CA can be configured only in conjunction with Active Directory. A Stand-alone CA can operate with or without Active Directory, but if Active Directory is not present, there can be only one SCS instance and the Stand-alone CA must be installed on the same platform as the SCS.

A PKI may have a hierarchy of Certificate Authorities, with subordinate CAs and a root CA. This is beyond the scope of this discussion. IT personnel who manage a facility that depends on PKI need in-depth knowledge of PKI protocols and supporting tools. The installation example later shows how to install a single tier Enterprise or Stand-alone CA.

## Support for Wireless Environments and Wired 802.1x

Intel AMT Releases 2.5, 2.6, and 4.0 run on mobile platforms. The SCS configures Intel AMT devices with these versions so that they can receive management traffic over wireless links. The SCS supports defining wireless profiles and 802.1x profiles. Intel AMT Releases 2.5, 2.6 and 3.0 and later releases also support wired 802.1x links. See [Configuring WiFi](#) for wireless profile definition, and [Configuring 802.1x](#) for 802.1x profile definition using the SCS console. Setup of wired 802.1x profiles and wireless profiles that authenticate using 802.1x is permitted only if the SCS is configured to integrate with Active Directory.

The SCS has been tested with the Cisco\* Aironet 1200 Access Point and the following RADIUS servers (authentication with EAP-GTC is for wired 802.1x only):

- Cisco ACS: With 802.1x EAP-TLS, EAP-PEAP, EAP-FAST/GTC, EAP-FAST/TLS and EAP-FAST/MS-CHAPv2
- Funk Odyssey: With 802.1x EAP-TLS, EAP-PEAP and EAP-TTLS
- Meetinghouse Aegis: With 802.1x EAP-GTC and EAP-TLS
- Microsoft IAS: With 802.1x EAP-TLS

## Protecting Against Platforms Masquerading as Intel AMT Devices

The SCS starts its setup and configuration process upon receipt of a “Hello” message from an Intel AMT device. If the SCS receives a request from an Intel AMT device that is recorded in the database as having completed setup, the request will be ignored. This protects against a rogue platform masquerading as an Intel AMT device waiting for setup. If the Intel AMT device was reset to the Factory Setup (pre-configuration) state by an application other than the SCS or by entering an **Un-provision** command using the ME BIOS extension, then the device must be removed from the SCS database before setup can take place. See [Preparing and Managing Platforms](#) for details on how to do this using the SCS Management Console.

# Part II

---

## Quick Start

This part contains the following chapters:

- SCS Console Flow
- Connecting to the SCS



# 2

---

## SCS Console Flow

This chapter provides a list of tasks that are usually required for setting up and configuring Intel AMT machines via the Intel SCS Console. Each step in the list of tasks refers you to the relevant chapter of the book where necessary.

### Specify Platform Configuration Parameters

If you are not using Intel® vPro™ Technology Activator Utility or a script for configuring Intel AMT machines, you need to enter configuration parameters to SCS for each AMT machine.

For details, see “Adding a Platform Definition” on page 67.

### Add SCS Users

This section describes how you add users who have the appropriate privileges to use and administer the SCS.

For details, see “Adding SCS Users” on page 93.

### Create Profiles

A profile allows configuration of multiple Intel AMT platforms with certain configuration properties. A profile defines the security settings of the communication with the platform, the network environment, and more.

For details on creating profiles, see “Creating a Profile” on page 29.

## **Specify Console Settings**

You can specify various settings that determine how the Console operates.

For details, see “Console Settings” on page 79.

## **Create USB Key with TLS-PSK Keys (if required)**

The Factory mode setup process can be simplified by using a USB key containing a file of PID/PPS pairs and replacement passwords, if the AMT machine’s BIOS supports this method.

For details, see “Exporting TLS-PSK Keys to a USB Drive” on page 98.

## **Configure Global Settings (if required)**

You can configure and view settings that apply to the SCS service.

For details, see “Viewing and Configuring SCS Services” on page 103.



# 3

---

## Connecting to the SCS

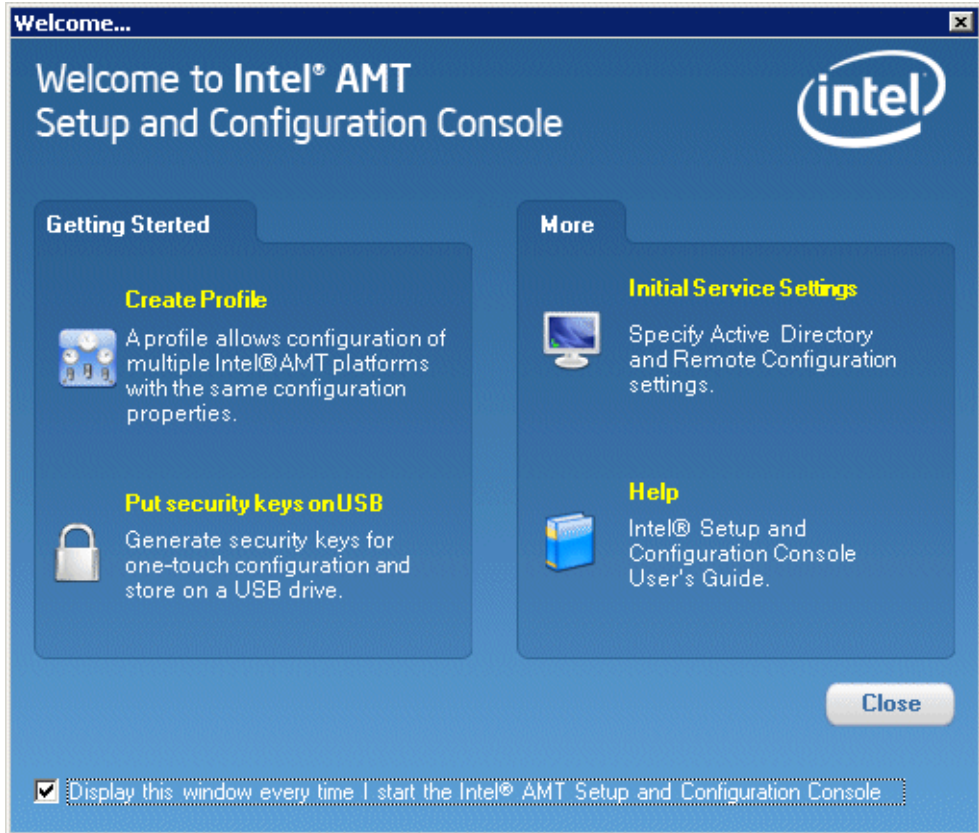
This chapter describes how to log on to the SCS Console.

### Logging On

You can log on to the SCS Console via the following methods:

- Choosing **Start > All Programs > Intel > Intel(R) AMT SCS Console**.
- Double-clicking the Console icon on your desktop.

After you have logged on, the Welcome window is displayed.



## Welcome Window

The Welcome window describes the tasks that generally need to be performed to enable using the SCS, and includes short-cuts to some of these tasks. (Note that all of the tasks are also available from the main Console window when you close the Welcome window.)

Click the appropriate link, or click **Close** to exit the Welcome page and view the main Console window. The various tasks you can perform via the Console are described in this book's subsequent chapters. The section below describes the tasks you can perform by clicking on the links in this page.

- Create Profile
- Put Security Keys on USB
- Initial Service Settings

### Create Profile

Click this link to open the profile wizard, which enables you to create a profile that defines the configuration properties for a group of Intel AMT platforms. You need to create a profile before you can configure platforms, or use the provided default profile.

For details on creating profiles, see “Creating and Changing Profiles” on page 27.

### Put Security Keys on USB

Click this link to generate security keys for one-touch configuration of Intel AMT platforms and store the keys on a USB drive.

For details on generating and storing security keys, see “Using USB Drives for TLS-PSK Keys” on page 95.

### Initial Service Settings

If you intend working with Active Directory, or if you intend using Remote Configuration, you need to configure the relevant service settings.

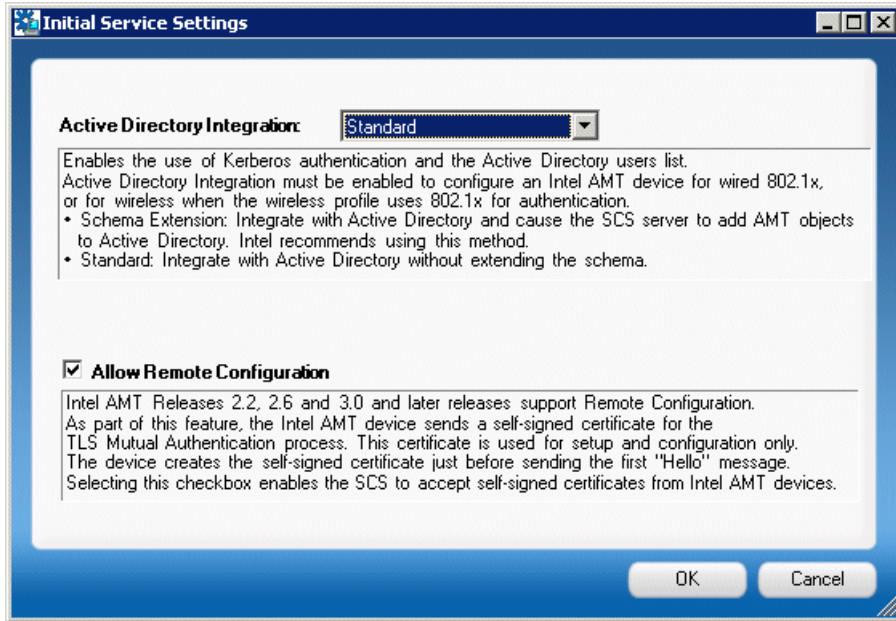
---

**Note:** If you do not specify the Active Directory or Remote Configuration settings in this window, you can do so later in the SCS Service Settings window. For details, see “Network Settings” on page 104.

---

To open a window that allows you to configure Active Directory or Remote Configuration settings:

- 1 Click **Initial Service Settings**. The Initial Service Settings window opens.



- 2 To specify the Active Directory settings, in the Active Directory Integration section, choose one of the following in the drop-down list:
  - **None**: For no integration with Active Directory.
  - **Schema Extension** (recommended by Intel if you intend working with Active Directory): Integrate with Active Directory and cause the SCS server to add AMT objects to Active Directory.
  - **Standard**: Integrate with Active Directory without extending the schema.
- 3 To allow Remote Configuration, check the **Allow Remote Configuration** box. For details on Remote Configuration, see "Remote Configuration" on page 133.

# Part III

---

## Console Operations

This part contains the following chapters:

- Creating and Changing Profiles
- Preparing and Managing Platforms
- Applying Operations to AMT Machines
- Managing SCS Users
- Using USB Drives for TLS-PSK Keys
- Viewing and Configuring SCS Services
- Viewing Log files
- Localization



# 4

---

## Creating and Changing Profiles

This chapter describes how to create and modify profiles.

This chapter includes the following sections:

- About Creating Profiles
- Creating a Profile
- Changing Network, Security or Power Management Settings
- Configuring ACL Settings
- Specifying Domains
- Configuring TLS Settings
- Configuring 802.1x
- Configuring WiFi
- Configuring CIRA (Client-Initiated Remote Access)
- Viewing and Editing a Profile's Properties

## About Creating Profiles

A profile allows configuration of multiple Intel AMT platforms with certain configuration properties. A profile defines the security settings of the communication with the platform, the network environment, and more.

The Console includes a wizard that you use to create a profile. The wizard creates a profile with default properties. After you create the profile, you can edit its properties to suit your needs.

---

**Note:** When you install the SCS, it includes a default profile for basic authentication using a random password.

---



## Creating a Profile

This section describes how to use the Profile wizard to create a default profile.

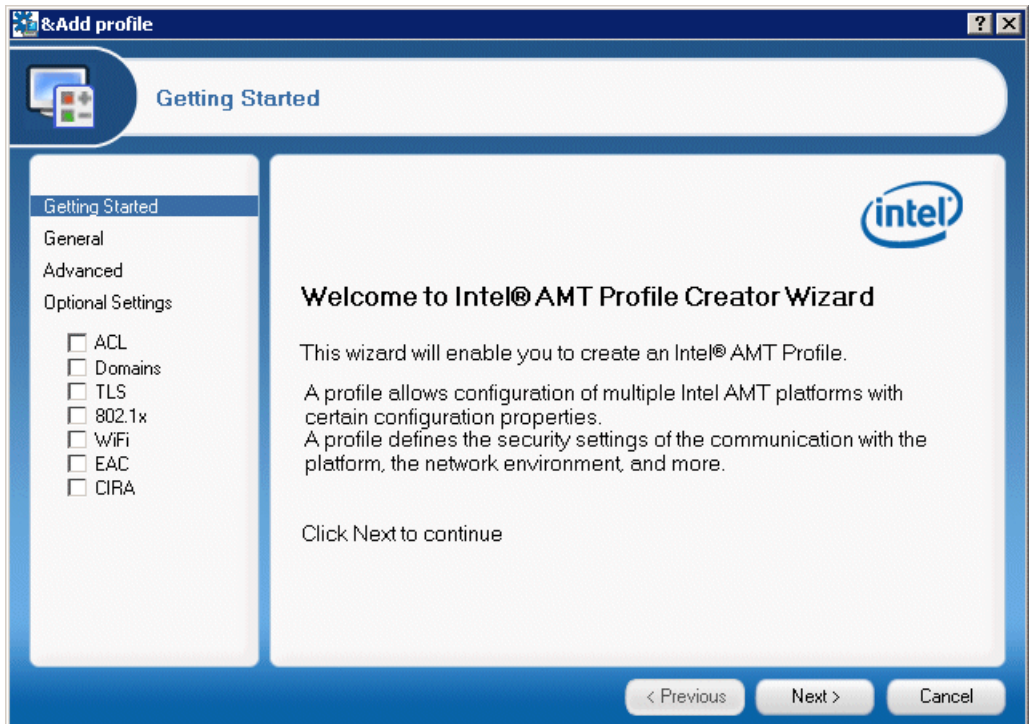
To create a profile:

- 1 In the Console tree, right-click the **Profiles** element and choose **Add Profile**.

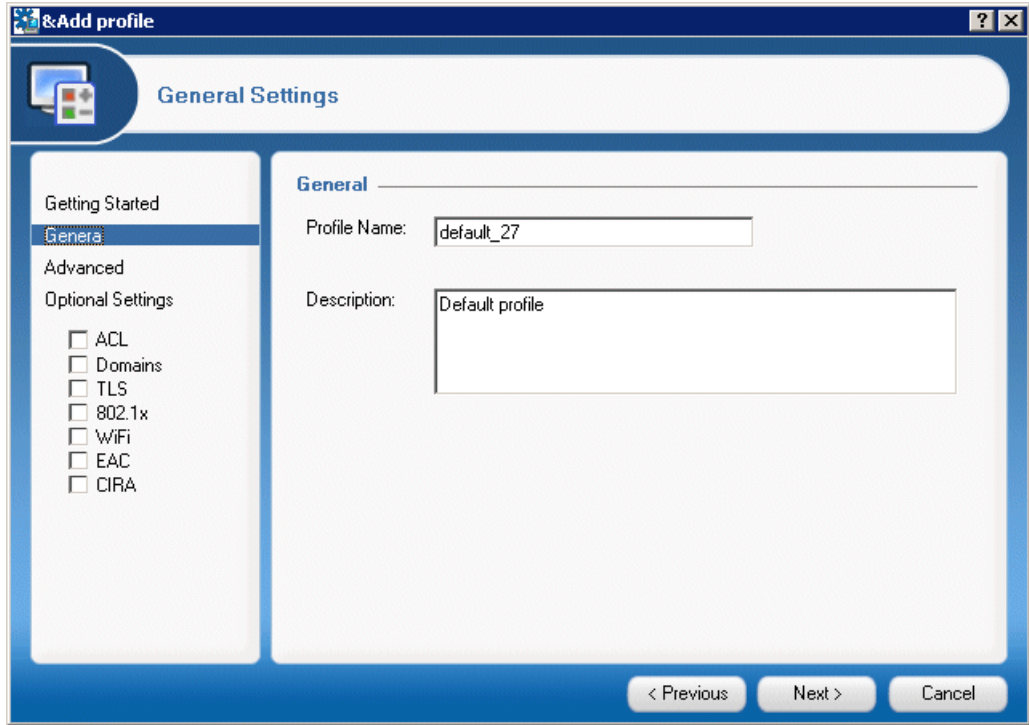
Alternatively, in the Welcome window, click **Create a Profile**.

The Profile Creator wizard opens.

- 2 Click **Next**. The New SCS Profile Wizard opens, displaying the Before You Begin section, which contains information on creating profiles.



- 3 In the Basic Settings section, click **General**.



### Profile Wizard General Settings Window

You use this window for specifying a profile's general settings.

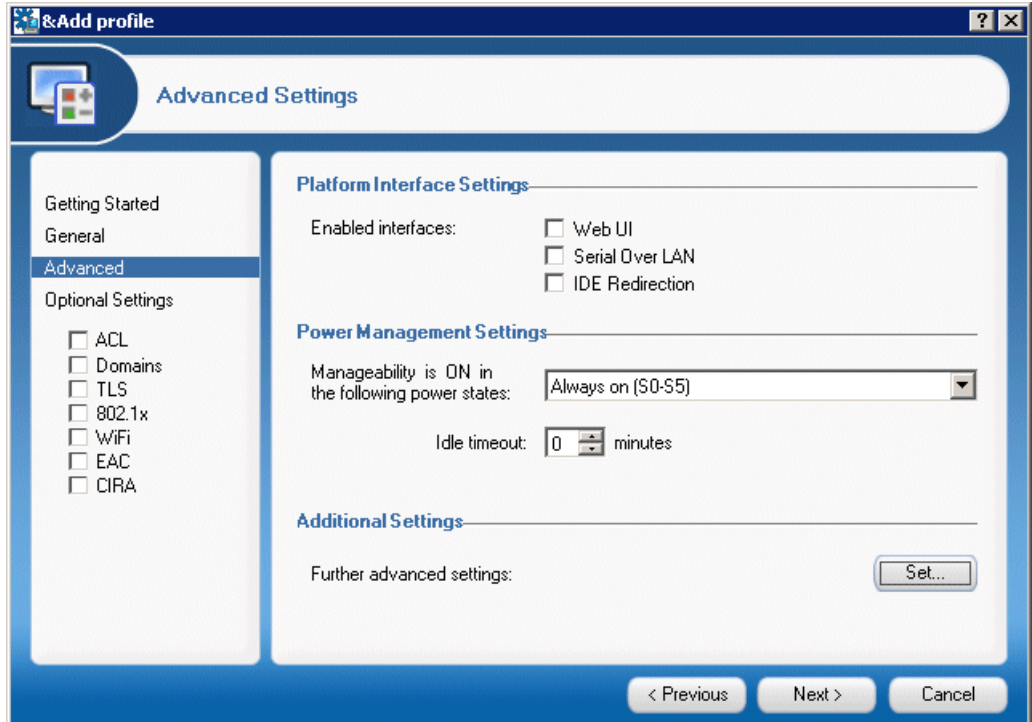
To specify the general settings:

- 1 Enter a name in the **Profile Name** field or accept the name provided by the Console.
- 2 Enter the Profile Description. This text field serves to describe the profile's properties.
- 3 In the **Optional Settings** section, check the relevant boxes, depending on the type of profile you want to create.

This is often all that you need to do to create a profile with default settings. To complete the profile, click **Finish**.

## Changing Network, Security or Power Management Settings

If you need to change or view the profile's default network, security or power management settings, click **Advanced** in the left navigation pane.



### Profile Wizard Advanced Settings Window

You use this window for specifying a profile's default network, security or power management settings.

#### Platform Interface Settings

In this section, you can change the values of the following parameters:

**Enabled interfaces:** Check one or more of the following:

**Web UI:** 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.

## Power Management Settings

In this section, you can change the values of the following parameters:

**Manageability is ON in the following power states:** 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.

**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 will remain operable when there is no activity. The device will return 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 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 will remain 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 will cause it to wake up and restart the timeout timer. This parameter should be set to three minutes at a minimum.

## Additional Settings

To view or edit additional settings, click the **Set** button. The Advanced Profile Settings window opens.

**Advanced profile settings**

**New MEBx password**

New password for certificate based configuration:

☒ Mask

**Configuration encryption mode**

Configuration encryption mode:

☒ Force encryption

☐ Force clear-text

☐ Allow encryption or clear-text

**Kerberos**

Kerberos clock tolerance:

**Network Settings**

☐ Use VLAN      Tag:

☐ Enable ping response

OK Cancel

## Advanced Profile Settings window

You use this window to configure the following properties:

**New MEBx password for certificate based configuration:** Enter and confirm the password used during Remote Configuration. The Remote Configuration process requires that the MEBx password be changed before the setup and configuration can complete.

**Configuration encryption mode:** Choose one of the following:

- **Force encryption:** When this box is checked, setup and configuration can be performed only on platforms that support encryption.
- **Force clear-text:** When this box is checked, setup and configuration can be performed only on platforms that do **not** support encryption.
- **Allow encryption or clear-text:** When this box is checked, setup and configuration can be performed on both types of platforms (encrypted and clear-text).

---

**Note:** Do not select **Force clear-text** or **Allow encryption or clear-text** if all platforms containing Intel AMT devices in the enterprise are supposed to support encryption. Use an unencrypted PSK only in cases where Intel® AMT does not support encryption due to import restrictions.

---

---

**Note:** If you specify **Force clear-text** or **Allow encryption or clear-text**, you cannot subsequently configure the machine to accept AMT operations that are transmitted to it using TLS.

---

**Kerberos 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.

## Network Settings

In this section, you can change the values of the following parameters:

- **Use VLAN:** If all the AMT platforms using the profile belong to a VLAN, check this box and specify the VLAN Tag Integer, used to distinguish between different VLANs.

---

**Note:** Make sure the VLAN settings are correct. If they are not, and you use a VLAN, the Intel AMT devices will not be accessible.

---

- **Enable ping response:** When this box is checked, the Intel AMT device will respond to a ping. (Default: Enabled)

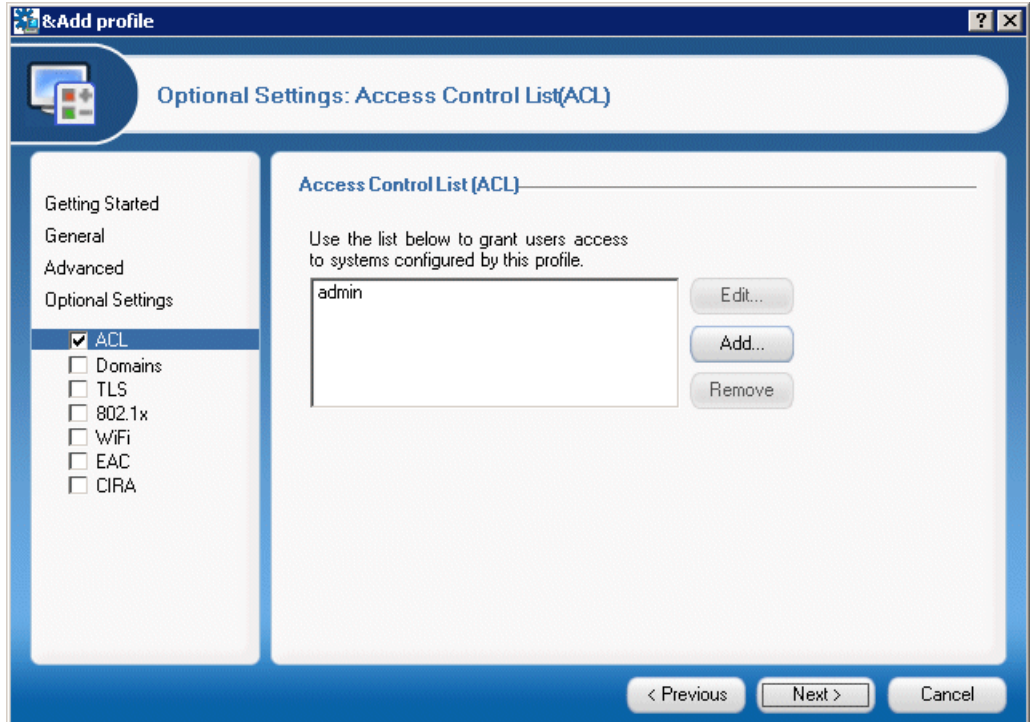
When you have made any necessary changes, click **Next**.

This is often all you need to do to create a basic profile with default parameters.

The subsequent windows depend on the boxes that you checked in the Profile Components section.

## Configuring ACL Settings

If you checked **ACL** in the Profile Components section, the wizard displays the Access Control List (ACL) settings.



### Access Control Settings Window

You use the Access Control Settings window to configure access control.

You use the Access Control List (ACL) settings to review users already associated with this profile and to add new users and define their access privileges. User identification and realm selection must be coordinated with the requirements and instructions of third-party Management Consoles.

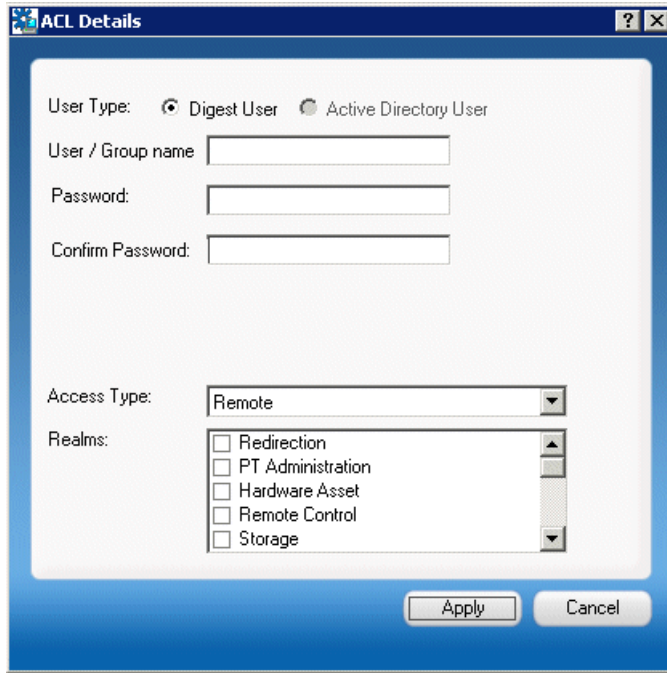
There are the following types of users:

- **Digest users:** Users that use digest authentication, which is password-based.
- **Active Directory users.**



To add a user:

- 1 Click **Add**. The ACL Details window opens.



## ACL Details Window

You use the ACL Details window to add a new user or group.

To create a digest user:

- 1 Select **Digest User** in the User Type section.
- 2 Enter the user name and password, and confirm the password.

The username and password will be the administrative username and password in the Admin ACL entry for all Intel AMT devices configured with this profile. A third-party Management Console application may have a pre-defined username and password for Intel AMT device administration. Those values should be used here.



To create an Active Directory user (possible only if the profile has Active Directory enabled):

- 1 Select **Active Directory User** in the User Type section.
- 2 Click the browse button. The Select User or Group dialog box is displayed.
- 3 Enter all or part of a user name. The user must be an individual for Digest ACL entries but can be a Group for a Kerberos ACL entry.
- 4 Click **Check Names**. The Intel SCS searches Active Directory and completes or confirms the user name.
- 5 Click **OK**.
- 6 **Randomize Password**: Checking this box means that only the SCS can use the admin ACL entry for managing the Intel AMT device.
- 7 Next specify an access type. This parameter defines user access, that is, 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.

In the Access Type section, choose one of the following:

- **Local**: The user can access the Intel AMT device only via the local host.
- **Remote**: The user can execute an action via the network.
- **Both**: The user can execute an action either locally or from the network (This option is not recommended).

Next select the realms that will be available to the user. The realms define specific functional capabilities (such as Redirection or PT Administration) available to this ACL entry. The following table lists the realms and their capabilities. Note that not all realms are available on all versions of Intel AMT.

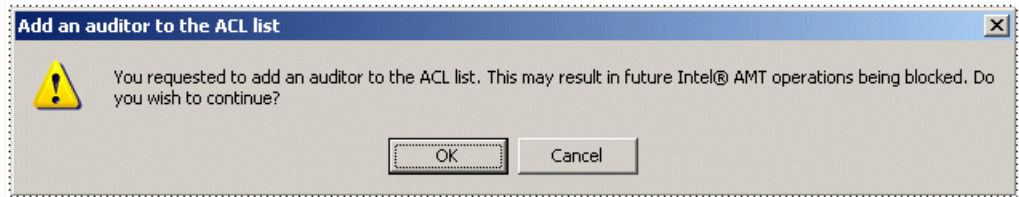
Realm	Capabilities	Comments
Redirection	Enables and disables the redirection capability and retrieves the redirection log. The redirection interface itself is a separate proprietary interface that does not depend on HTTP/SOAP. See the Redirection Library Design Guide.	
PT Administration	Manages security control data, such as Access Control Lists, Kerberos parameters, Transport Layer Security, Configuration parameters, power saving options and power packages.	A user with PT Administration Realm privileges has access to all realms.
Hardware Asset	Used to retrieve information about the hardware inventory of the platform.	
Remote Control	Enables powering a platform up or down remotely. Used in conjunction with the Redirection capability to boot remotely.	
Storage	Used to configure, write to and read from non-volatile user storage. The actual commands are in the Storage Library.	
Event Manager	Allows configuring hardware and software events to generate alerts and to send them to a remote console and/or log them locally.	

Realm	Capabilities	Comments
Storage Administration	Used to configure the global parameters that govern the allocation and use of non-volatile storage.	
Agent Presence Local	Used by an application designed to run on the local platform to report that it is running and to send heartbeats periodically.	
Agent Presence Remote	Used to register Local Agent applications and to specify the behavior of Intel AMT when an application is running or stops running unexpectedly.	
Circuit Breaker	Used to define filters, counters, and policies to monitor incoming and outgoing network traffic and to block traffic when a suspicious condition is detected (The System Defense feature).	
Network Time	Used to set the clock in the Intel AMT device and synchronize it to network time.	
General Info	Returns general setting and status information. With this interface, it is possible to give a user permission to read parameters related to other interfaces without giving permission to change the parameters.	
Firmware Update	Used only by OEMs via Intel-supplied tools to update the Intel AMT firmware.	
EIT	Implements the Embedded IT service.	

Realm	Capabilities	Comments
Local User Notification	Provides alerts to a user on the local interface	
Endpoint Access Control	Returns settings associated with NAC posture.	
Endpoint Access Control Admin	Configures and enables the NAC posture.	
Event Log Reader	Allows definition of a user with privileges only to read the Intel AMT system log.	
Security Audit Log	Allows a system auditor to monitor critical events.	
User Access Control	Groups several ACL management commands into a separate realm to enable users to manage their own passwords without requiring admin privileges.	
WoX	Provides support for additional "Wake on..." capabilities.	
Danbury	Provides support for remote configuration and management of Danbury hardware disk encryption technology.	

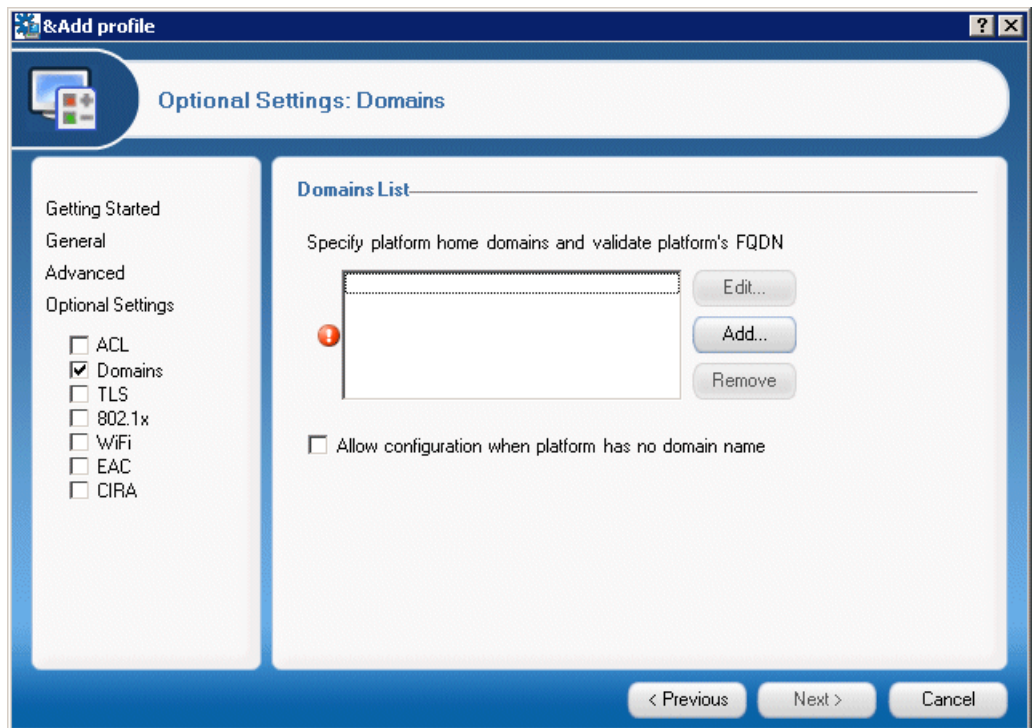
The **admin** user account has access to all realms, including **Security Audit Log**. Once an ACL entry has been given access to the **Security Audit Log** realm, only a user with **Security Audit Log** privileges can change this user's privileges. The **admin** user cannot change the user's privileges.

Assigning the **Security Audit Log** realm causes the following message to be displayed:



## Specifying Domains

If you checked **Domains** in the Profile Components section, the wizard displays the domain settings.



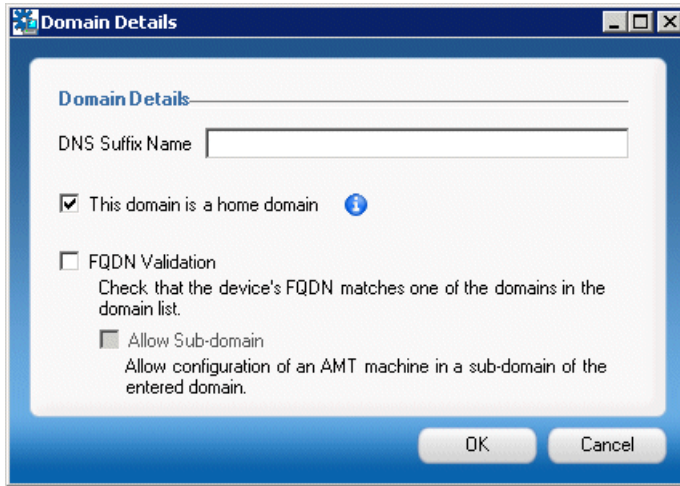
The Domains List box defines the domains from which an AMT machine can initiate configuration by the SCS.

To allow configuration when the platform has no domain name:

- Check the box next to **Allow configuration when platform has no domain name**.

To add a domain to the list:

- 1 Click **Add**. The Domain Details window opens.



## Domain Details Window

You use the Domain Details window to add a domain to the list of domains from which an AMT machine can initiate configuration by the SCS.

- 1 In the **Domain Name** field, enter the name of the domain.
  - 2 Check or clear the following boxes as needed:
- **This domain belongs to the home domain list:** Checking this box has the following effects:
    - **CIRA (Remote access):** If the AMT machine is not in a home domain, the machine will attempt to use CIRA to connect to the SCS (if CIRA is defined).
    - **WiFi:** If the AMT machine 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 AMT machine will use the host's WiFi settings as long as the access point is in one of these domains.

---

**Note:** In a multi-level domain environment, if the AMT systems in the environment have LMS version 2.6 or later installed, you do not need to specify separately all the child domains as home domains; they will be automatically included with the parent domain.

To find out which version of LMS is installed on an AMT machine, locate the **LMS.exe** file in the machine's **C:\Program Files\Intel\AMT** directory, right-click the file to display the Properties window, and click the **Version** tab. If the version is older than 2.6 and you require this functionality, contact your Intel support team.

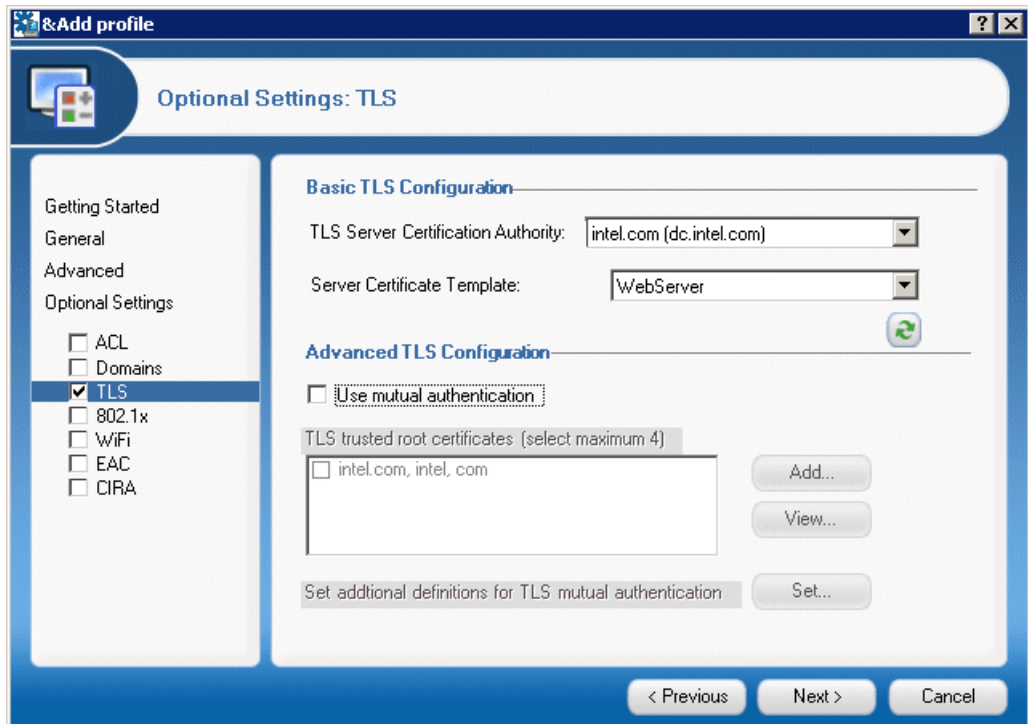
---

- **FQDN Validation:** When this box is checked, 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 used for setup and configuration.
- **Allow sub-domains** (enabled if the Allow Configuration box is checked): If this box is checked, SCS will allow configuration (using this profile) of an AMT machine in a sub-domain of the domain entered in the Domain Name field. For example, if the domain name is **intel.com**, and the **Allow sub-domains** box is checked, AMT machines in **europa.intel.com** can also be configured.

## Configuring TLS Settings

When TLS is enabled, the Intel AMT device will require a server certificate used to authenticate itself with other applications. If mutual TLS authentication is enabled, any applications that interact with the device will need to supply client certificates that the device will use to authenticate the applications. When Use TLS is selected, configure the interfaces to indicate which will use TLS or mutual TLS or neither.

If you checked **TLS** in the Profile Components section, the wizard displays the TLS settings.



### TLS Settings Window

You use the TLS Settings window to specify the settings for TLS authentication.

- 1 Choose a certification authority from the **TLS Server Certification Authority** list.
- 2 Choose a certificate template from the **WebServer Template** list.



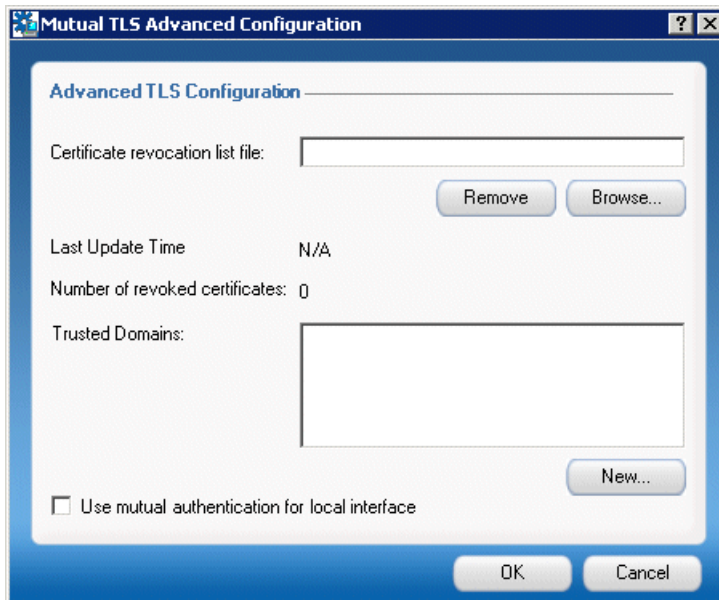
- 3 To use TLS mutual authentication, check the **Use Mutual Authentication** box.
- 4 Check one or more of the trusted root certificates in the **TLS trusted root certificates** list (up to a maximum of four certificates).

---

**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 EAC posture signing and CIRA. 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.

---

- 5 To configure advanced TLS settings for mutual authentication, click **Set** in the TLS Configuration window. The Mutual TLS Advanced Configuration window opens.



### Mutual TLS Advanced Configuration Window

You use the Mutual TLS Advanced Configuration window to configure advanced TLS settings for mutual authentication.

- 1 In the **Certificate revocation list file** field, enter (or browse to and select) the CRL. The CRL is a list of entries that indicate which certificates have been revoked. The CRL contains Certification Authority URLs and the serial numbers of revoked certificates. (See CRL XML Format for the XML file format.) Enter information about the list into the Description field.

**Last Update Time:** When the CRL was last updated.

**Number of revoked certificates:**

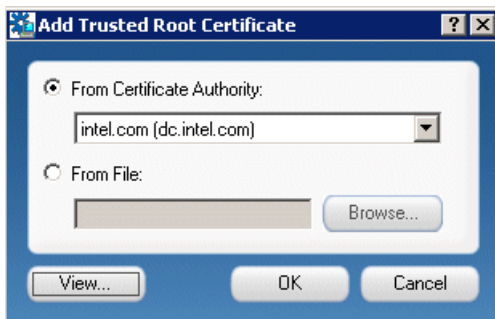
- 2 The **Trusted Domains** field lists the Fully Qualified Domain Name suffixes that will be used by mutual authentication. The Intel AMT device will validate that any client certificates used by the SCS or Management Consoles have one of the listed suffixes in the certificate subject. If no FQDN suffixes are defined, the Intel AMT device will not validate client certificate subject names.

To add a domain to the list, click **New** and specify the domain in the Add New Domain Entry window.

- 3 To cause host communications with the Intel AMT device to require TLS (with or without mutual authentication), check **Use mutual authentication for local interface**.

To add a trusted root certificate:

- 1 In the TLS Settings window, click **New** in the Advanced TLS Configuration section. The Add Trusted Root Certificate window is displayed.



## Add Trusted Root Certificate Window

You use the Add Trusted Root Certificate window to add a trusted root certificate to the list of certificates that will be used for authentication.

---

**Note:** You can only add a certificate from a Certification Authority that is self-signed (that is, there is no Certification Authority above it). You cannot add a certificate from a subordinate Certification Authority.

---

- 1 Choose a certification authority from the list  
or  
Click **From File**, then click the **Browse** button and choose a certificate.
- 2 To view details of the chosen certificate, click **View**.
- 3 Click **OK** to add the certificate and close the Add Trusted Root Certificate dialog box.

## Configuring 802.1x

---

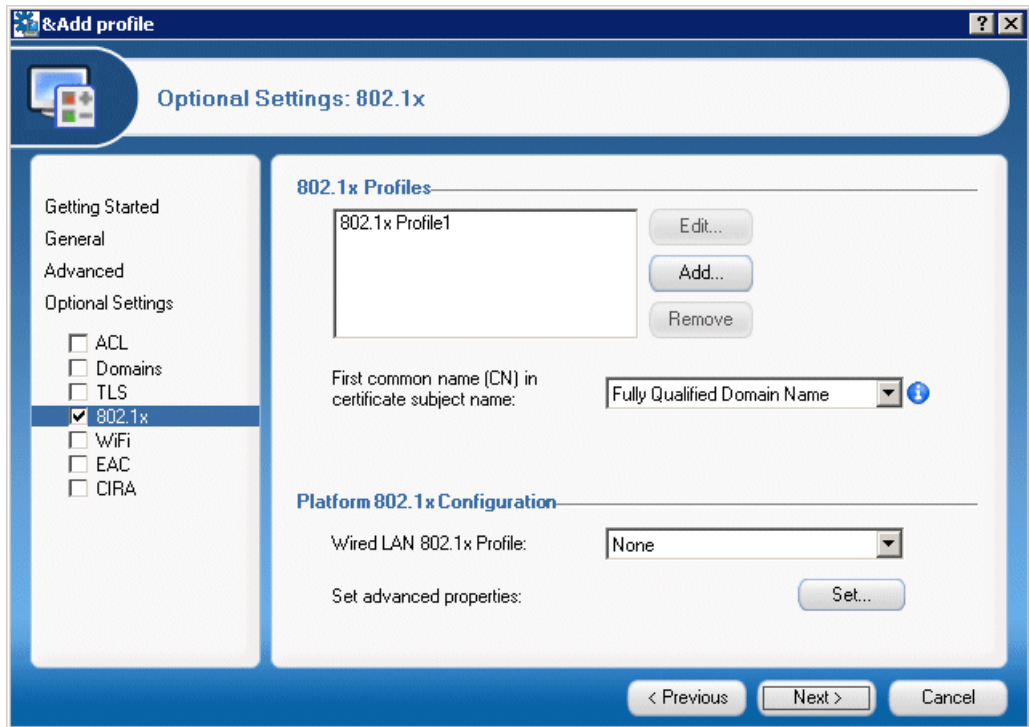
**Note:** Configuring 802.1x is available only for Intel AMT Releases 2.5, 2.6, and 3.0 and later.

---

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 apply to either wired or wireless connections.

Use the Wired 802.1x tab to select an optional 802.1x profile, used by the Intel AMT device to authenticate on a wired LAN when the device is active in S3, S4 or S5 power states. Note that Active Directory integration must be enabled in the SCS Service Settings window (Service Network Integration tab) to be able to configure an Intel AMT device with a wired 802.1x profile.

If you checked **802.1x** in the Profile Components section, the wizard displays the 802.1x settings.



## 802.1x Profile Settings Window

The 802.1x Profile Settings Window displays the available (but not necessarily used) 802.1x profiles and their properties.

- 1 If the list is empty, click **Add** to open the 802.1x Profile window and create a profile. For details on creating an 802.1x profile, see “Adding an 802.1x Profile Component” on page 51.
- 2 Choose a profile from the **Wired LAN 802.1x Profile** list.

- 3 Client certificates used to validate Intel AMT with RADIUS servers or other external servers must be in a format compatible with those servers. In particular, the Common Name must be in the form that the server expects. When the SCS requests a certificate for an Intel AMT device, the SCS-generated certificate request will use the selection made here for the Common Name in the request.

---

**Note:** The Funk RADIUS server expects a host name. Cisco ACS and Microsoft IAS require a SAM account name. All others tested with the SCS accept an FQDN.

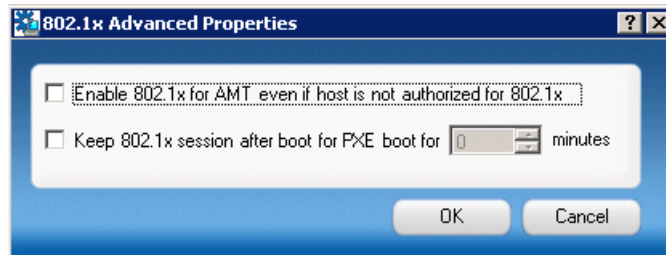
---

In the **First common name (CN) in certificate subject name** list, specify the format that the AMT machine expects for the first CN in a certificate. This can be one of the following:

- **Fully-Qualified Domain Name:** FQDN of the Intel AMT device
- **Host Name:** Host name of the platform (available if integration with Active Directory is enabled)
- **SAM Account name:** Active Directory account name for the AMT object (available if integration with Active Directory is enabled)

To configure advanced 802.1x properties:

Click **Set**. The 802.1x Advanced Properties window opens.



## 802.1x Advanced Properties Window

You use the 802.1x Advanced Properties window to configure the following 802.1x properties:

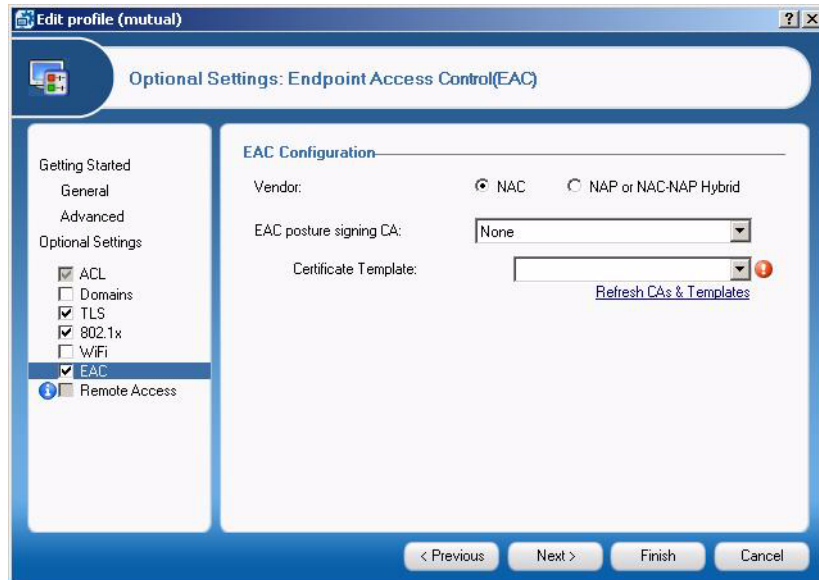
- **Enable 802.1x for AMT even if host is not authorized for 802.1x:** If you check this box, manageability traffic is enabled even if the host is unable to complete 802.1x authentication to the network.
- **Keep 802.1x session open after PXE boot for .... minutes:** If you check this box, the 802.1x session is kept alive after a PXE boot for the number of minutes that you specify (up to 1440 minutes—24 hours). This is the period 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 will be forced to zero.

## Specifying EAC Definitions

If the 802.1x profile's protocol is one of the EAP-FAST protocols, you can use NAC authentication along with the RADIUS server to authenticate the AMT device. If the 802.1x profile's protocol is one of the PEAP definitions, you can specify NAP or NAC-NAP hybrid authentication.

To specify EAC definitions:

- 1 In the Profile Components section, select the **EAC** checkbox. The EAC Settings window opens.



## EAC Settings Window

You use this window for specifying EAC settings.

- 1 In the Vendor section, choose **NAC** or **NAP or NAC-NAP Hybrid**.
- 2 In the **EAC posture signing CA** list, choose the certificate authority to use for issuing a client certificate for EAC posture signing.
- 3 In the **Certificate Template** list, choose the template to use when issuing the certificate.
- 4 Select **Refresh CAs & Templates** if there are new CAs or templates to use.

## Adding an 802.1x Profile Component

To create an 802.1x profile component:

- 1 In the Profiles element, right-click **802.1x Profiles** and choose **Add 802.1x Profile**.

The 802.1x Profile window opens.

The screenshot shows the '802.1x Profile' window with the following configuration:

- General**
  - Profile Name: 802.1x Profile2
  - Protocol: EAP-FAST (MS-CHAP v2)
- Authentication**
  - Client Certificate Authority: None
  - Client Certificate Template: (empty)
  - Trusted Root Certificate (for Radius Server authentication): (empty)
  - Buttons: View..., New...
  - ☐ Roaming Identity
  - First common name (CN) in certificate subject name: Fully Qualified Domain Name
- Radius Server Domain Name Verification**
  - ☒ Do not verify Radius Server certificate subject name
  - ☐ Radius Server name (FQDN): (empty)
  - ☐ Radius Server domain suffix: (empty)

Buttons at the bottom: OK, Cancel, Apply.

## Add 802.1X Profile Window

You use this window for creating a new 802.1x profile component.

To create a new component:

- 1 In the Profile Name field, enter a name for the new 802.1x profile.



- 2 In the Protocol field, select from one of the available options. The client and server authentication methods enabled on the 802.1x Profile tab vary according to the protocol selected:

	Client Authentication Options	Server Authentication Options
EAP-TLS	Client Certificate required	Trusted root for RADIUS server certificate required
EAP-TTLS (MS-CHAP v2)	Client Certificate optional, Roaming Identity optional	Trusted root for RADIUS server certificate required
EAP-PEAP (MS-CHAP v2)	Not required, Roaming Identity optional	Trusted root for RADIUS server certificate required
EAP (GTC)	Not required	Not required
EAP-FAST (MS-CHAP v2)	Client Certificate required, Roaming Identity optional	Trusted root for RADIUS server certificate required
EAP-FAST (TLS)	Client Certificate required, Roaming Identity optional	Trusted root for RADIUS server certificate required
EAP-FAST (GTC)	Client Certificate required, Roaming Identity optional	Trusted root for RADIUS server certificate required

- 3 In the Trusted Root Certificate field, select a trusted root certificate for RADIUS Server authentication.
- 4 To add a trusted root certificate to the list, click **New**. The Add Trusted Root Certificate dialog box is displayed.
- 5 Choose a certificate from the list in the **From Certificate Authority** list  
or  
Click **From File**, then click the **Browse** button and choose a certificate.
- 6 To view details of the chosen certificate, click **View**.

- 7 Click **OK** to close the Add Trusted Root Certificate dialog box.

The client authentication options require defining a source for a client certificate for authenticating an Intel AMT device to a RADIUS server.

To define a source for a client certificate:

- 1 In the Client Certificate Authority list, select a certificate authority.
- 2 In the Client Certificate Template list, select a template defined for creating the appropriate client certificate. Note that this should be a template where the subject name is supplied in the request and the usage is Client Authentication. For information about creating a template for 802.1x client certificates, see *Defining a New Template for an Enterprise CA* in the *Intel® Active Management Technology Setup and Configuration Service Installation Guide*.

---

**Note:** Defining a template requires an Enterprise CA, which requires the presence of Active Directory.

---

---

**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 EAC posture signing and CIRA. 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.

---

- 3 To enable roaming, check the **Roaming Identity** box. The user will have an identity of **Anonymous**.

For RADIUS server domain name verification, choose one of the following:

- To use the RADIUS Server's FQDN, click **RADIUS Server Name** and enter the FQDN in the adjacent field.
- To use the RADIUS Server's domain suffix, click **RADIUS Server Domain Suffix** and enter the domain name suffix of the RADIUS server subject name in the adjacent field.

- To not use RADIUS server domain name verification, click **Do not verify RADIUS server certificate subject name**.

## Configuring WiFi

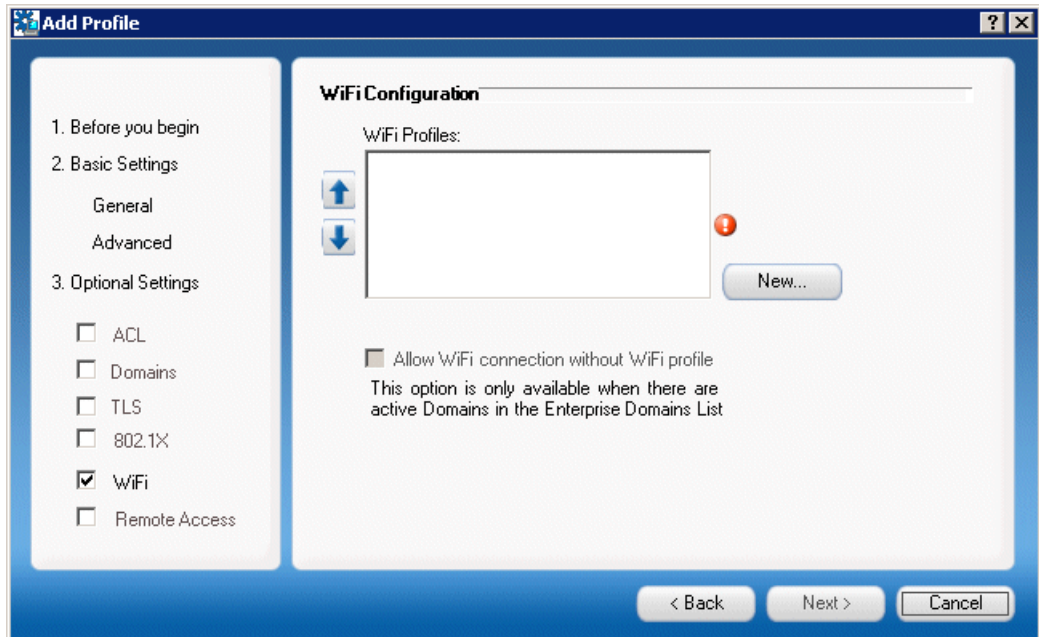
A wireless profile defines which protocol will be used between an Intel AMT device and a wireless access point. If the Intel AMT device is to receive manageability messages over a wireless connection, there must be a wireless profile installed on the device that corresponds with the wireless profile active on the host. The profiles conform to IEEE 802.11i.

---

**Note:** Intel AMT must be integrated with Active Directory to use 802.1x profiles.

---

If you chose WiFi in the Profile Components section, the wizard displays the WiFi settings.



## WiFi Profile Settings Window

In the WiFi Profiles list, choose one or more (up to 4) of the displayed WiFi profiles. If the list is empty, you need to create a new profile component.

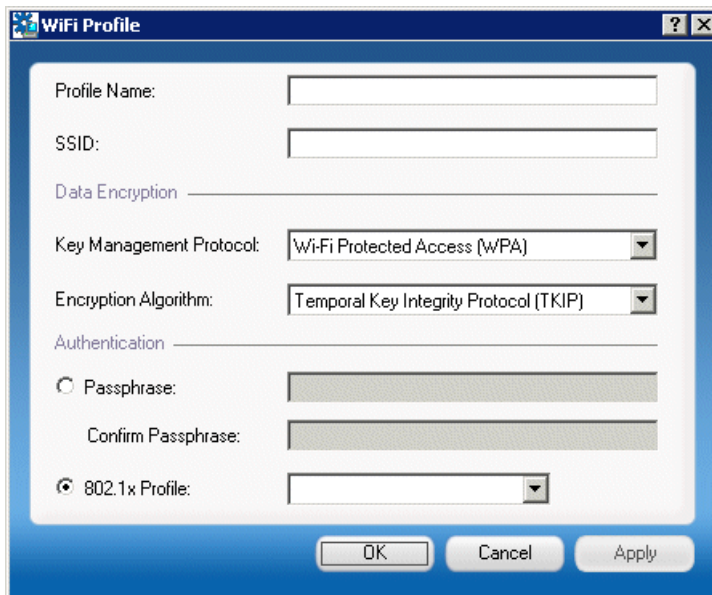
To allow WiFi connection even without a profile (using the host's WiFi settings):

Check the **Allow WiFi connection without profile** box.

To create a WiFi profile component:

- 1 In the WiFi Profiles settings window, click **New**.

The Add New WiFi Profile window opens.



The screenshot shows the 'WiFi Profile' configuration window. It includes the following elements:

- Title Bar:** 'WiFi Profile' with a help icon (?) and a close icon (X).
- Profile Name:** An empty text input field.
- SSID:** An empty text input field.
- Data Encryption:**
  - Key Management Protocol:** A dropdown menu currently showing 'Wi-Fi Protected Access (WPA)'.
  - Encryption Algorithm:** A dropdown menu currently showing 'Temporal Key Integrity Protocol (TKIP)'.
- Authentication:**
  - Passphrase:** A radio button followed by an empty text input field.
  - Confirm Passphrase:** An empty text input field.
  - 802.1x Profile:** A checked radio button followed by an empty dropdown menu.
- Buttons:** 'OK', 'Cancel', and 'Apply' buttons at the bottom right.

## Add New WiFi Settings Window

You use the Add New WiFi window to create a WiFi profile component.

To create a WiFi profile component:

- 1 **Profile Name:** Enter a name for this profile.

- 2 **SSID:** Enter an optional Service Set ID: a 1 to 32 character string naming a specific wireless LAN.
- 3 **Data Encryption:** Select a **Key Management Protocol** (WPA or RSN) and an **Encryption Algorithm** (TKIP or CCMP). These choices must correspond to the settings used in the specific wireless LAN environment.
- 4 **Authentication:** Either enter a Passphrase in the **Passphrase** field or select an 802.1x profile from the **802.1x** list. If you need an 802.1x profile but no profile is listed, click **New** to create an 802.1x profile. (For details on creating 802.1x profiles, see “Configuring 802.1x” on page 47.)

Once the 802.1x profile has been created, it appears in the **802.1x** list. Select the profile. For details, see “Viewing and Editing a Profile’s Properties” on page 63.

---

**Note:** Intel AMT Release 2.5 requires a strong passphrase: It must be at least eight characters and contain an upper-case letter, a lower-case letter, numbers, and one of the @ # \$ % ^ & \* ! symbols at a minimum. The SCS does not validate for a strong passphrase. Intel AMT Release 2.6 requires only that the passphrase be at least eight printable ASCII characters.

---

## Configuring CIRA (Client-Initiated Remote Access)

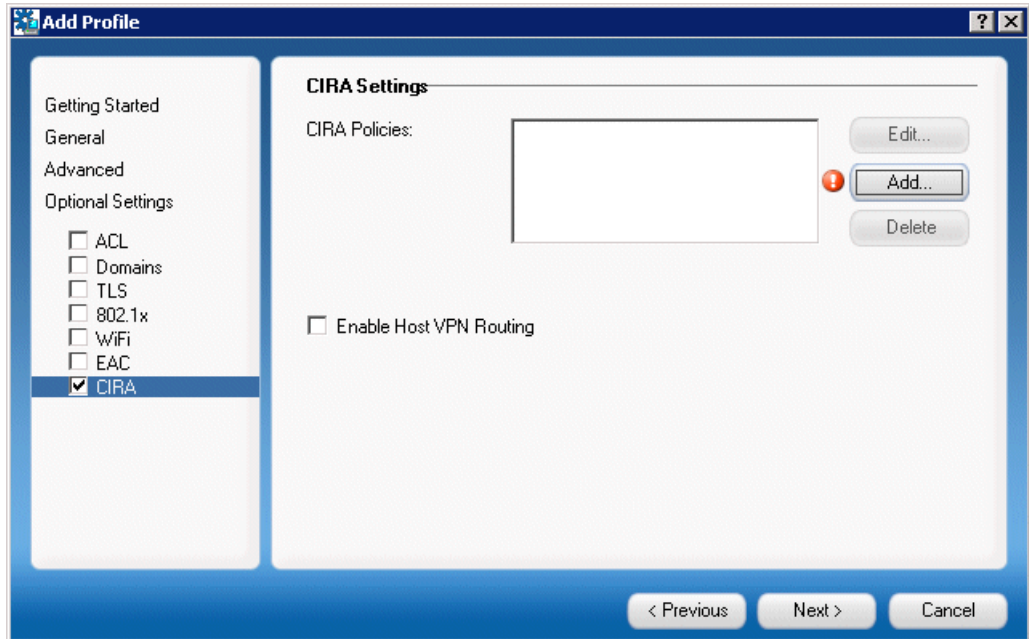
Intel AMT Release 4.0 and later releases support CIRA (client-initiated remote access). CIRA allows a platform containing Intel AMT located outside an enterprise to connect to management consoles inside the enterprise. The connection is accomplished via a Management Presence Server (MPS) located in the 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 CIRA to work, the Intel AMT platform must first be configured by the SCS when it is inside the enterprise with the information needed to connect with the MPS. The CIRA Settings window is used to enter the necessary parameters.

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.

The MPS connection parameters are defined separately.

If you chose CIRA in the Profile Components section, the wizard displays the CIRA settings window:



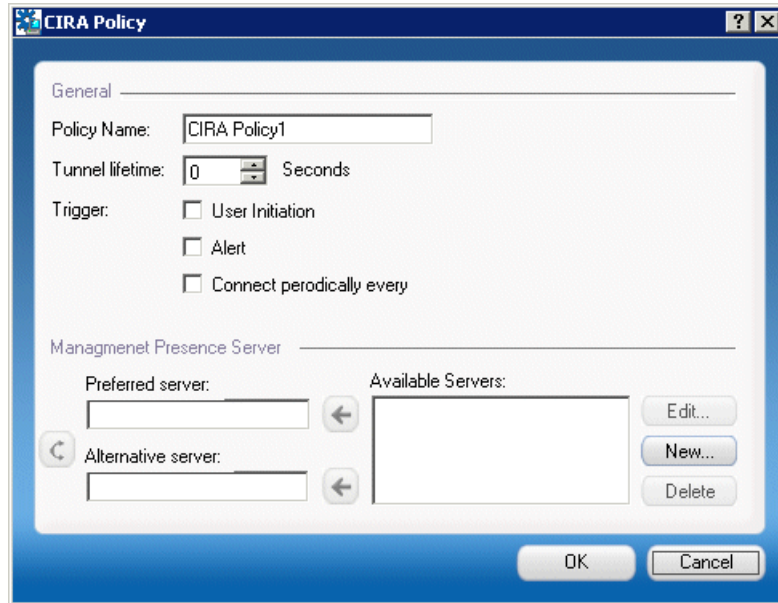
## CIRA Settings Window

The CIRA Settings window contains the following:

- **CIRA Policies list:** Choose one or more (up to 3) of the displayed CIRA profiles. If the list is empty, you need to create a policy. (See below.)
- **Enable Host VPN Routing:** When this box is checked, Intel AMT devices will accept management traffic over a Virtual Private Network connection when Intel AMT detects that the platform is operating outside the enterprise network.

To create a new CIRA policy:

- 1 In the Profiles element, right-click **CIRA Policies** and choose **Add CIRA Policy**. The Add/Edit CIRA Policy dialog box is displayed.



## Add/Edit CIRA Policy Window

You use the CIRA Policy window to create a new CIRA policy.

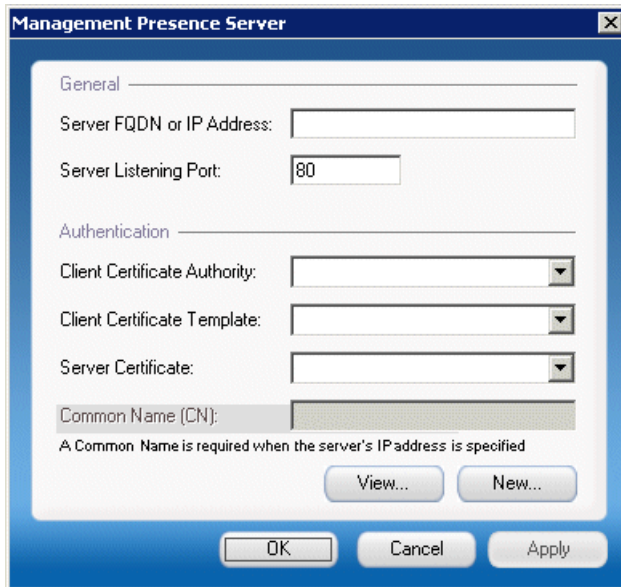
To create a CIRA policy:

- 1 In the Policy Name field, enter a descriptive name for the policy.
- 2 In the Tunnel Lifetime field, enter 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.

- 3 In the Trigger section, select the trigger or triggers associated with this policy. A particular trigger type can be selected in only one policy.
  - **User initiation:** the Intel AMT device establishes a tunnel with the MPS when the user initiates a connection request.
  - **Alert:** The device establishes a connection when an event occurs that generates an alert addressed to the network interface.
  - **Connect periodically:** The device connects to the MPS based on the **Seconds Between Connections** interval.
- 4 In the Management Presence Servers box, 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 listed in the **Preferred server** field. If that connection does not succeed, the device tries to connect to the server listed in the **Alternative server** field, if one was specified.

To add a new Management Presence Server specification:

- 1 Click **New**. The Management Presence Server dialog box is displayed.



The image shows a Windows-style dialog box titled "Management Presence Server". It has a blue title bar with a close button (X) in the top right corner. The dialog is divided into two sections: "General" and "Authentication".

**General section:**

- "Server FQDN or IP Address:" followed by a text input field.
- "Server Listening Port:" followed by a text input field containing the number "80".

**Authentication section:**

- "Client Certificate Authority:" followed by a dropdown menu.
- "Client Certificate Template:" followed by a dropdown menu.
- "Server Certificate:" followed by a dropdown menu.
- "Common Name (CN):" followed by a text input field.

Below the "Common Name (CN)" field, there is a note: "A Common Name is required when the server's IP address is specified".

At the bottom of the dialog, there are three buttons: "View...", "New...", and "OK". The "View..." and "New..." buttons are located below the "Common Name (CN)" field. The "OK", "Cancel", and "Apply" buttons are located at the very bottom of the dialog.



## Management Presence Server Window

You use the Management Presence Server window to add a new Management Presence Server specification.

To add a Management Presence Server specification:

- 1 In the **Server FQDN or IP Address** field, enter the FQDN or IP address of the Management Presence Server.
- 2 In the **Server Listening Port** field, enter the Port that the Management Presence Server listens on for connections from Intel AMT devices.
- 3 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.

In the **Client Certificate Authority** field, choose the Certificate Authority that the AMT platform will use to request a certificate that the MPS can authenticate.

- 4 In the **Client Certificate Template** list, select a template defined for creating the appropriate client certificate. Note that this should be a template where the subject name is supplied in the request and the usage is Client Authentication. For information about creating a template for 802.1x client certificates, see *Defining a New Template for an Enterprise CA* in the *Intel® Active Management Technology Setup and Configuration Service Installation Guide*.

---

**Note:** Defining a template requires an Enterprise CA, which requires the presence of Active Directory.

---



---

**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 EAC posture signing and CIRA. 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.

---

5

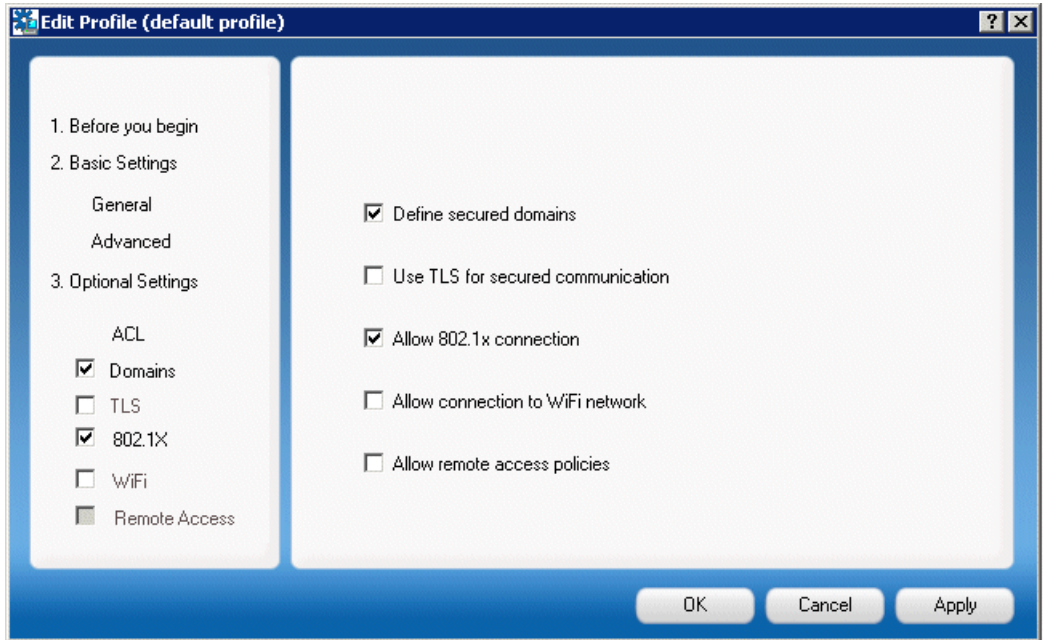
- 6 In the **Server Certificate** field, choose the root certificate of the Certificate Authority that the MPS will use to authenticate itself to the AMT platform.
- 7 If you entered an IP address in the Server FQDN or IP Address field (see step 1 on page 61), you need to enter the FQDN in the Common Name field. (If you entered the FQDN in the Server FQDN or IP Address field, the Common Name field is disabled.)
- 8 To add a trusted root certificate to the list, click **New**. The Add Trusted Root Certificate dialog box is displayed.
- 9 Choose a certificate from the list in the **From Certificate Authority** list  
or  
Click **From File**, then click the **Browse** button and choose a certificate.
- 10 To view details of the chosen certificate, click **View**.
- 11 Click **OK** to close the Add Trusted Root Certificate dialog box.

## Viewing and Editing a Profile's Properties

You can view a profile's properties and edit them.

To view or edit a profile's properties:

- 1 In the tree, click **Profiles**. The available profiles are listed in the right pane.
- 2 Double-click the profile that you want to edit. The Edit Profile window opens.



- 3 In the left pane, click the section whose settings you want to edit. The relevant window opens.

---

**Note:** The windows that open are similar to the ones that open when you use the wizard to create a profile. For details on the specific settings window, see “Creating a Profile” on page 29.

---

- 4 Make your changes.

- 5 Click **Apply** or **OK** to apply your changes.

# 5

---

## Preparing and Managing Platforms

This chapter describes the various operations you can perform on AMT platforms via the SCS Console.

This chapter contains the following sections:

- Adding Device Configuration Information to SCS
- Searching for Platforms
- Adding a Platform Definition
- Viewing and Changing Platform Settings
- Creating and Viewing Collections
- Deleting Collections
- Exporting Lists of Machines

## Adding Device Configuration Information to SCS

The SCS needs identification information for each Intel AMT device to know its FQDN, which Profile to use and where to put the AMT object in Active Directory. The identifying parameter for a device and the platform that it is on is the platform UUID. Entering the information manually in an enterprise environment is not practical on a large scale. Also, the FQDN will change as a machine is moved around in the enterprise and assigned to different individuals. The SCS supports multiple methods for loading configuration information, each with its uses, advantages and disadvantages.

### Source of Configuration Information: Database or Script

The SCS can be configured to locate Intel AMT device configuration information in one of two ways: either from within the SCS database or via a script. When the SCS receives a "Hello" message from a device it will look in the SCS database for a configuration entry matching the UUID in the "Hello" message. If there is no match, and there is no script, the SCS will revisit the queued "Hello" message periodically to see if an entry was added to the database. If the script option was selected, the SCS will activate a script to find the necessary information, given the UUID and the source IP in the "Hello" message. When the SCS receives the configuration from the script, it stores the information in the database.

### Scripting Option

This option acquires the configuration information using a script if the required parameters are not in the New Intel AMT database table. The SCS runs a script that retrieves the parameters from an external source

The SCS distribution and documentation include sample scripts and directions for several of these options. See “Using a Script to Import Intel AMT Configuration Properties” on page 153.

### Adding device information to the SCS database manually

This is the simplest approach but it is the most difficult for IT personnel. They have to manually enter the UUID along with the other parameters into the New Intel AMT table.

### Adding device information to the SCS database using the SOAP API

The SOAP API has a method called `AddServiceNewAMTProperties` that adds an entry to the SCS database table. An external management console can acquire the

platform information using scripts, its own database, or a local agent, and pass the information to the SCS either before or after the Intel AMT device starts sending "Hello" messages.

## Searching for Platforms

You can view all the platforms in the SCS that match part or all of a hostname.

To view specific platforms:

- 1 Choose **Actions > Find Platform** or use any other option to initiate the search. The Search Platform window opens.

### Search Platform Window

This window allows you to search for one or more specific platforms.

- 1 Select one of the fields in the search filter and select a condition and the parameter for the filter. You may use the Add button to add other fields to the conditions. This process creates an AND query. To delete a condition use the 'X' button.
- 2 Click **Search**.
- 3 The platforms that match the query that you entered are displayed in the Search Results section.
- 4 To view or change any of a platform's settings, double-click the relevant platform.

## Adding a Platform Definition

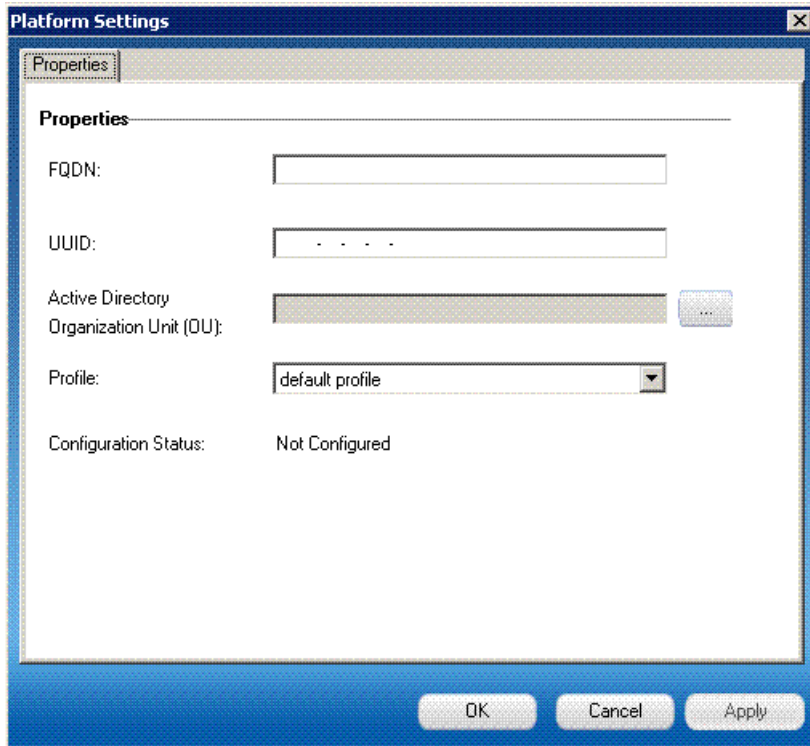
If you are not using the Intel® vPro™ Technology Activator Utility or a script to insert the configuration information about each device in the SCS database, you use the Console to do this.

You define the platform in the Console and enter the configuration information in the platform definition.

To define a platform:

- 1 In the Console tree, right-click the **All Platforms** element and choose **New Platform**.

The Platform Settings window is displayed.



## Platform Settings Window

You use the Platform Settings window to define a platform's settings.

To define a platform's settings:

- 1 Enter the Intel AMT machine's FQDN and UUID in the relevant fields.
- 2 Click the Browse button adjacent to the Active Directory Organization Unit (OU) field and choose the OU to which the Intel AMT system will belong.
- 3 From the Profile list, choose the profile that you want to use to configure the Intel AMT system.
- 4 Click **OK** to save your settings. The new platform definition appears in the Platforms element.



## Deleting Platform Information and/or Configuration Properties

You can delete a platform's definition from the SCS.

To delete a platform definition:

- 1 In the Console tree, click the **All Platforms** element. All the platforms are displayed in the right pane.
- 2 Right-click the platform that you want to delete and choose **Delete Platform** (or use any other option to delete).
- 3 From the Platform Delete window select the information you want to delete: platform information and/or the platform configuration properties, according to the information available for the selected platform.

## Viewing and Changing Platform Settings

You can view the settings of any platform that appears in the Console. Some of the settings can be changed.

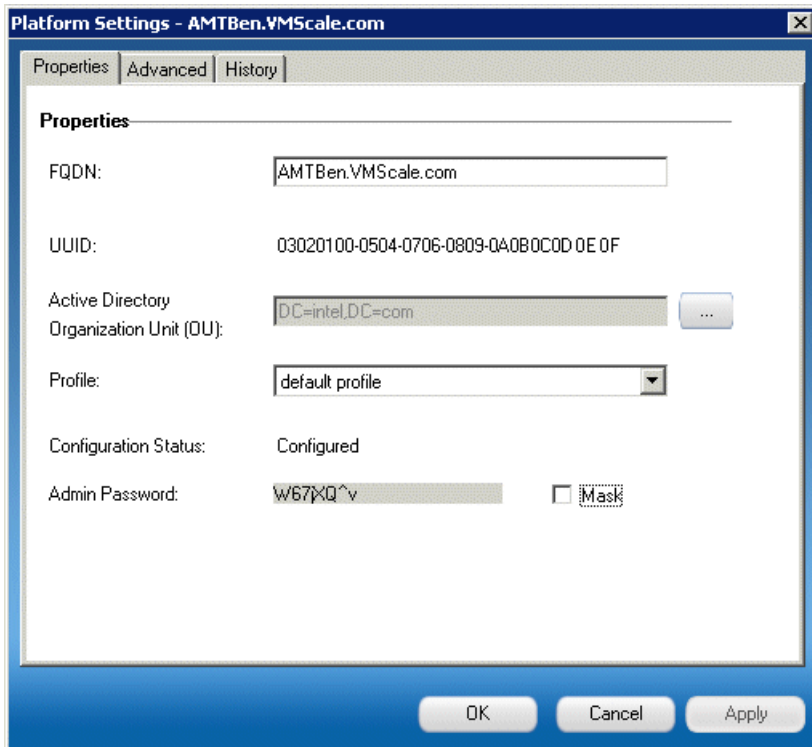
---

**Note:** If you change any settings and then click **Apply** or **OK**, the SCS applies the new settings to the AMT platform.

---

To view or change a platform's settings:

- 1 In the right pane, double-click the platform. The Platform Settings window is displayed.



## Platform Settings Window

You use this window to view or change a platform's settings.

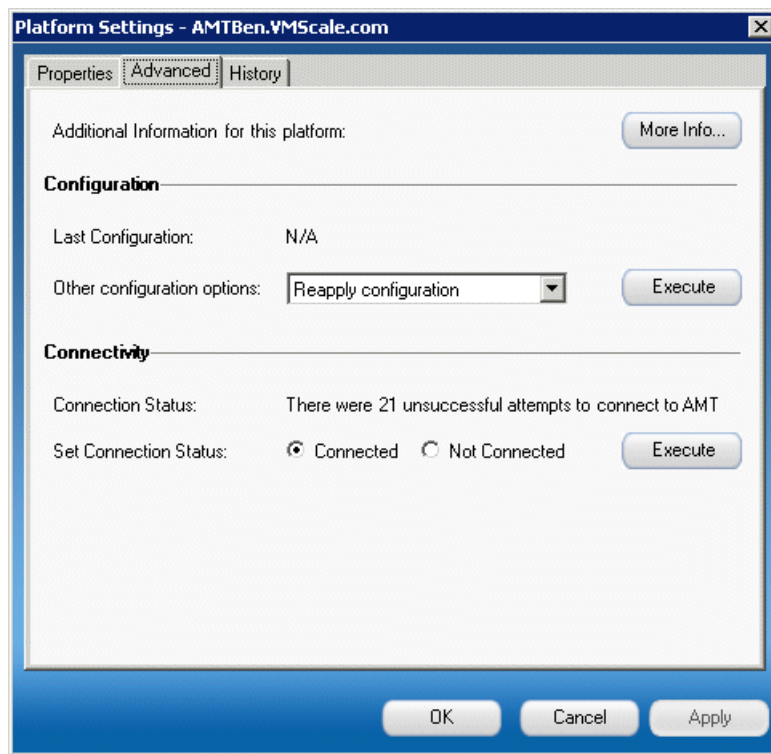
This window contains the following tabs:

- Properties Tab (Platform Settings Window)
- Advanced Tab (Platform Settings Window)
- History Tab (Platform Settings Window)

## Properties Tab (Platform Settings Window)

The Properties tab displays the current information for the FQDN, UUID, Active Directory OU and Profile, and the platform's configuration status.

- 1 To change parameters of the platform:
  - **FQDN:** Type the platform's new FQDN.
  - **Profile:** Choose another profile from the Profile drop-down list.
- 2 To view additional information about the platform, click the **Advanced** tab.



## Advanced Tab (Platform Settings Window)

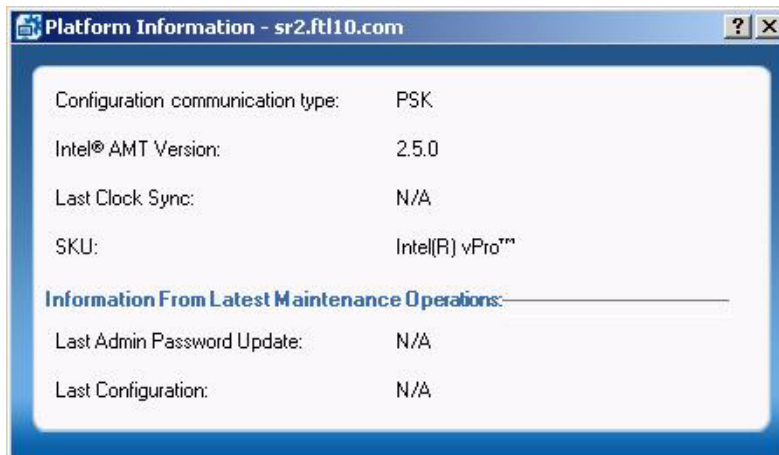
This tab displays the following information about the platform:

- **Last Configuration:** Date and time the platform was last configured

- **Other Configuration Options:** Choose one of the following operations to apply to the platform and then click the adjacent **Execute** button:
    - **Reapply configuration.** For details, see “Reapplying Configurations” on page 82.
    - **Reset configuration.** For details, see “Resetting Configurations” on page 84.
    - **Reset for factory defaults.** For details, see “Resetting a Platform or Collection to Factory Default Values” on page 85.
  - **Connection Status:** Information on connection history (for example, the number of attempts that were made to connect to the platform).
  - **Set Connection Status:** The current status of the platform in the SCS database (**Connected** or **Not Connected**) is displayed. To change the status, choose the new status and click the adjacent **Execute** button.
- 3 In the Advanced tab, to view additional platform information, click **More Info**. The Platform Information window is displayed, providing additional information about the platform.

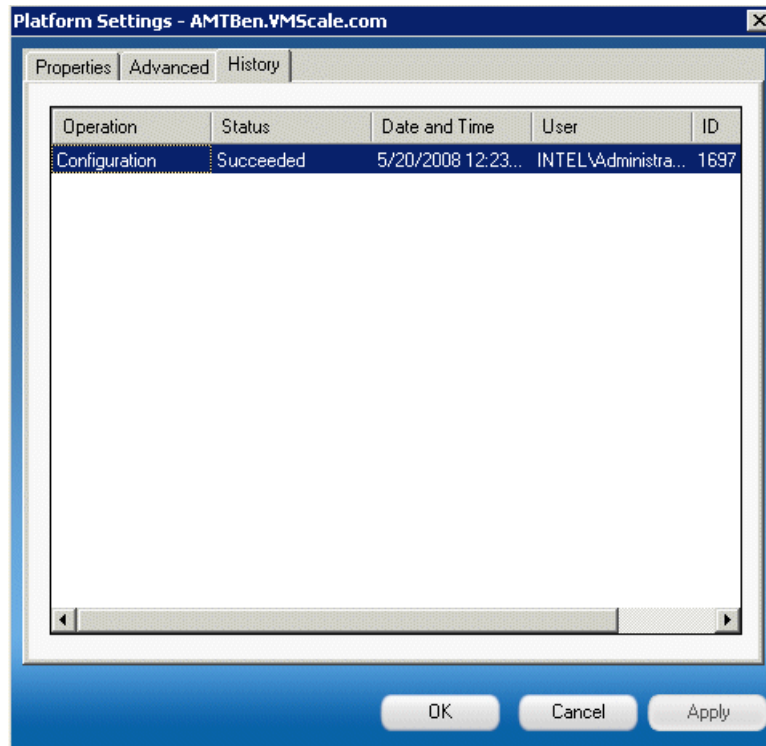
## Platform Information Window

This window displays the following information about the platform:



- **Configuration Communication Type:** The type of communication (PSK....) used for configuration.
- **Intel AMT Version:** The AMT version of the platform.
- **Last Clock Sync:** The date and time the platform's clock was synchronized with the SCS clock.
- **SKU:** The platform's SKU.
- **Last Admin Password Update:** The date and time the platform's Admin password was last changed during maintenance operation.
- **Last Configuration:** The date and time the platform was last configured during maintenance operations.

1 To view the platform's history, click the **History** tab.



## History Tab (Platform Settings Window)

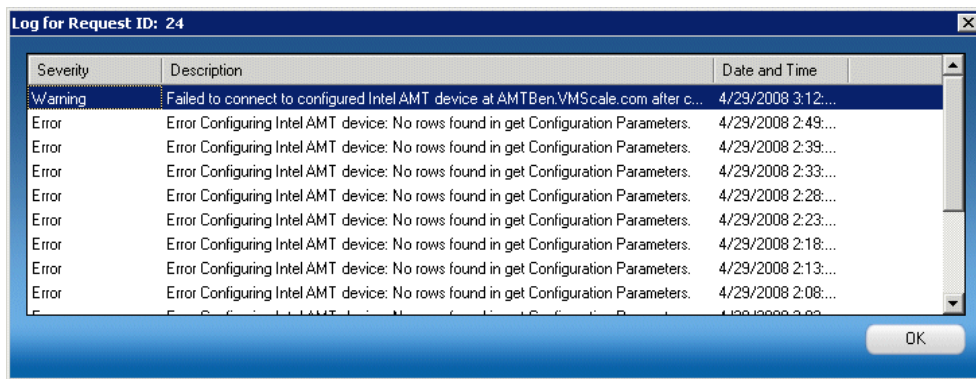
The following information is displayed about each operation:

- **Operation:** Type of operation
  - **Status:** Status of the operation (**Configured**, **Unconfigured**, **In Configuration**)
  - **Date and Time:** Date and time the operation was executed
  - **User:** The user account running the SCS service that performed the operation
  - **ID:** ID of the request
- 2 To display a list of the log messages that preceded an operation, double-click the operation, or select the operation and click **View**.

## Log for Command Window

The Log for Command window displays the following information about each log message:

- Severity
- Description
- Date and Time



- 3 To view additional information about a specific message, double-click the message, or select the message and click **View**. The Event Details window opens with more information about the event that caused the log message.

- 4 To save any changes and apply them to the AMT platform, click **Apply** or **OK**. To exit the window without making any changes, click **Cancel**.

## Creating and Viewing Collections

The SCS Console allows you to create a filter that defines a group of platforms. This filter is known as a *sub-collection*. Once you have defined a sub-collection, you can view all its platforms and apply various AMT operations to them. When you apply an operation to a collection, the operation is applied to all the AMT systems that the collection includes.

To create a sub-collection:

- 1 In the Console tree, right-click the **All Platforms** element and choose **Create Platform Sub-Collection**.

The Platform Collection window is displayed.

### Create Platform Collection Window

You use the Create Platform Collection window to define a collection of platforms on which you can perform AMT operations

To create a platform collection:

- 1 Enter a name for the collection in the Collection Name field.
- 2 In the left-most list, choose the filter type. The filter type defines the values in the remaining list fields.

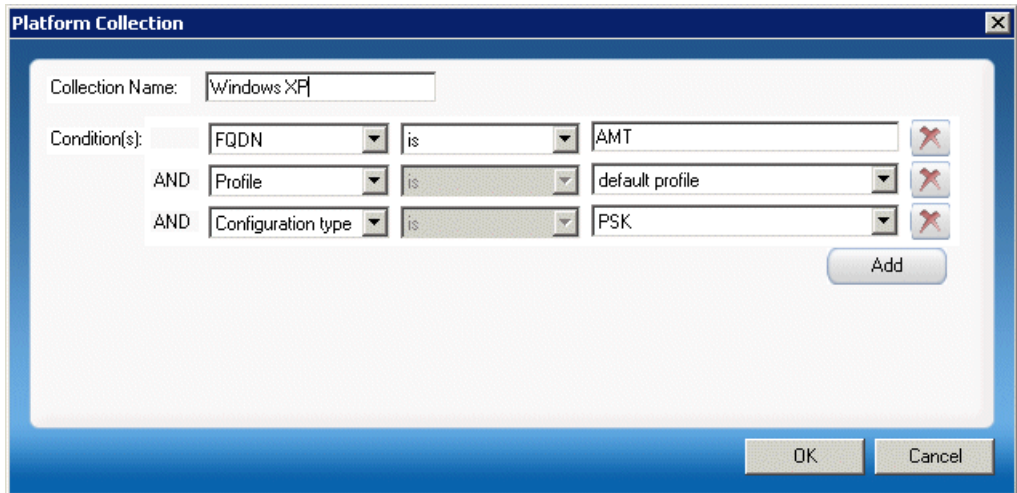
The following table describes the available choices for each type of filter:

	Operator	Operand
FQDN	<ul style="list-style-type: none"> <li>• is</li> <li>• contains</li> <li>• starts with</li> <li>• ends with</li> </ul>	Any string comprising part of a host name
Configuration date	on or after	A date chosen from the calendar that appears when you click the field's down-arrow
UUID	is	A string comprising part of a UUID
Configuration type	is	<ul style="list-style-type: none"> <li>• PSK</li> <li>• Remote Configuration</li> </ul>
Status	is	<ul style="list-style-type: none"> <li>• Not Configured</li> <li>• Configured</li> <li>• In Configuration</li> <li>• Setup</li> </ul>
Profile	is	A profile chosen from the list in the right-most field

- 3 Choose or enter the appropriate values in the center and right-most list fields.

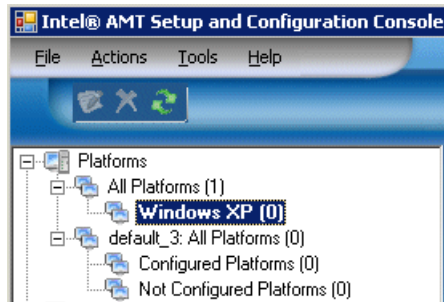


- 4 To add another filter condition, click **Add** and enter the relevant values. Continue adding filter conditions until the filter is complete.



- 5 Click **OK**.

The collection appears in the Platforms section.



To display all the platforms that meet the filter criteria:

Click the collection.

## Deleting Collections

You can delete collections. (This does not delete the platform definitions.)

To delete a collection:

In the left pane, right-click the collection and choose **Delete Platform Collection**.

The collection is deleted and no longer appears in the Console.

## Exporting Lists of Machines

You can create a list of AMT platforms as an XML file.

To create a list of AMT platforms:

- 1 Right-click the relevant collection or right-click **All Platforms**.
- 2 Click **Export List of Platforms**.

The Save As window is displayed.

- 3 Specify the location where you want to save the XML file and click **Save**.

# 6

## Console Settings

This chapter describes the various settings that you can configure that determine the way the SCS Console operates.

This chapter contains the following sections:

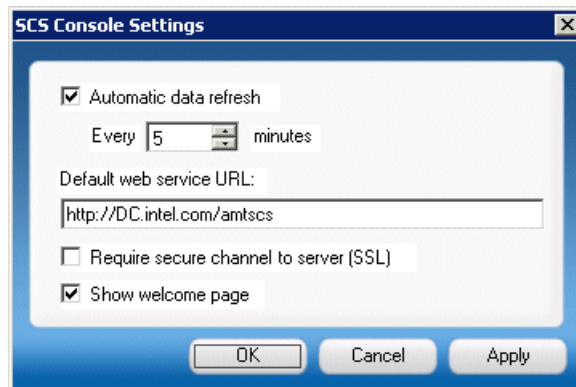
- Specifying Console Settings

### Specifying Console Settings

Before you use the SCS Console, you should check the default settings and modify them if necessary.

To view or modify the Console settings:

- 1 Choose **Tools > Console Settings**. The Console Settings window opens.



## Console Settings Window

You use the Console Settings window to determine the way the SCS Console operates.

The window contains the following fields:

- **Automatic data refresh:** Checking this box causes the data displayed in the Console to be updated automatically. After checking the box, type or select the number of minutes in the refresh interval.

The data is also updated every time a window is displayed (entered) by the user, even if automatic refresh is not enabled.

To refresh the data manually, click **F5**.

- **Default web service URL:** The default URL path, including the virtual directory, used by the Console to connect to the SCS. For example, if **provisionserver.yourenterprise.com** is the FQDN of the IIS host of the web service, and **AMTSCS** is the virtual directory of the SOAP web service in the IIS host, enter **http://provisionserver.yourenterprise.com/AMTSCS** or **https://provisionserver.yourenterprise.com/AMTSCS**, depending on whether you are using TLS.

If the web server expects a port number other than port 80, include the port number after the FQDN. For example, if the port is 123, you would specify the URL as follows:

**https://provisionserver.yourenterprise.com:123/AMTSCS**

- **Require secure channel to server (SSL):** Checking this box causes the Console to connect to the SCS service via TLS (https). If this box is not checked, both http and https can be used for communications.
- **Show Welcome page:** Show the Welcome page when the Console is opened.

# 7

---

## Applying Operations to AMT Machines

This chapter describes how to apply operations to one or more specified AMT platforms.

This chapter describes how to perform the following operations (some operations can be applied to collections as well as to individual platforms):

- Reapplying Configurations
- Resetting Configurations
- Resetting a Platform or Collection to Factory Default Values
- Updating ACLs
- Setting CRLs
- Setting Power Policies
- Synchronizing Clocks
- Setting Connection Status
- Authorizing Setup and Configuration

## Reapplying Configurations

You can reapply configurations to platforms and collections. When you reapply a configuration, the SCS applies the current values of a platform's profile to the platform.

---

**Note:** Data transmitted when reapplying configurations data may contain sensitive information. If the AMT device is in non-TLS mode, reapplying the device's configuration will cause all the data to be sent unencrypted.

---

This operation first removes all settings from the Intel AMT device and then applies all the current settings in the profile associated with the device in the configuration parameters table. It also updates the AMT object in Active Directory based on the profile settings.

---

**Note:** If you are integrated with Active Directory, reapplying a configuration causes the AMT object in Active Directory to be overwritten by a new one. This requires any management console that is trying to access this AMT system to renew its Kerberos ticket. If the management console tries to access the machine whose configuration has been reapplied via the old ticket, the connection will fail.

---

---

**Note:** When there is an enabled active wireless profile on the Intel AMT device, that profile cannot be disabled by an external command, since this might break the only manageability connection with the device. Also, if the wireless profile depends on a certificate, that certificate cannot be deleted. When you reapply a configuration, if there is a wireless profile with the same name as the active profile in the configuration profile associated with the device, the SCS will define a profile with the same name with an appended underscore and send it to the device. For example, if the active profile is named WP1, the SCS will install a profile named WP1\_.

Continuing the above example, after a configuration has been reapplied, and the wireless link is eventually dropped, the next wireless connection attempt may fail. This occurs because the Intel AMT device will try to establish a link using WP1 and the RADIUS server may try to authenticate using Active Directory. The credentials in the old profile WP1 will not match the new Active Directory credentials created during reapplying. After WP1 fails, the device tries to connect using the next wireless profile (WP\_) and will succeed as this profile has up-to-date credentials

---

**To reapply a platform's configuration:**

- 1 Select the platform.
- 2 Choose **Actions** or right-click the platform.
- 3 Choose **Configuration > Reapply Configuration**.

The SCS reapplies the current profile values to the platform.

**To reapply configuration to all platforms in a collection:**

- 1 Right-click the collection and choose **Collection Configuration > Reapply Configuration**.

The SCS reapplies the current profile values to each platform in the collection.

## Resetting Configurations

This operation disables the Intel AMT device. It deletes all data on the Intel AMT device except the PID, PPS, admin ACL settings, host name, domain name, and provisioning server IP and port number.

Following reset, the device immediately starts sending “Hello” messages, causing the SCS to set up and configure the device according to the profile associated with it.

---

**Note:** If auditing was enabled on the Intel AMT device, you cannot reset the device unless the auditor has permitted configuration reset.

---

To reset a platform's configuration:

- 1 Select the platform.
- 2 Choose **Actions** or right-click the platform.
- 3 Choose **Configuration > Reset Configuration**.

The SCS deletes the platform's Setup and Configuration information.

To reset configuration of all platforms in a collection:

Right-click the collection and choose **Collection Configuration > Reset Configuration**.

The SCS deletes the Setup and Configuration information from each platform in the collection.



## Resetting a Platform or Collection to Factory Default Values

This operation disables the Intel AMT device and leaves it without any Setup and Configuration parameters. It differs from the Reset Configuration operation in that this operation deletes all data from the Intel AMT device. The Intel AMT device is not functional after this operation. If it is configured for "bare metal" remote configuration, the device will open the network interface and start sending "Hello" messages. Because the PID-PPS are removed from the AMT during reset to factory defaults, the PSK configuration is not possible in this state.

---

**Note:** If auditing was enabled on the Intel AMT device, you cannot reset the device unless the auditor has permitted configuration reset.

---

To reset a platform to the factory defaults:

- 1 Select the platform.
- 2 Choose **Actions** or right-click the platform.
- 3 Choose **Configuration > Reset to Factory Defaults**.

The SCS deletes the platform's Setup and Configuration information and causes the AMT functionality to cease operating.

To reset all platforms in a collection to the factory default settings:

Right-click the collection and choose **Collection Configuration > Reset to Factory Defaults**.

The SCS deletes the Setup and Configuration information from each platform in the collection and causes the AMT functionality of each platform to cease operating.

## Updating ACLs

This operation updates the list of Intel AMT users and their access privileges, according to the ACL entries in the profile associated with each device.

To update a platform's ACL:

- 1 Select the platform.

2 Choose **Actions** or right-click the platform.

3 Choose **Operations > Set ACL**.

The Console updates the list of Intel AMT users and their access privileges.

To update the ACL for all the platforms in a collection:

Right-click the collection and choose **Collection Operations > Set ACL**.

## Setting CRLs

You can update a platform's list of revoked certificates (the Certificate Revocation List—CRL).

To update the CRL for a platform:

1 Select the platform.

2 Choose **Actions** or right-click the platform.

3 Choose **Operations > Set CRL**.

The Console updates the CRL for the platform.

## Setting Power Policies

You can update a platform's power policy according to the parameters defined in the profile. For details on power management settings, see [“Power Management Settings” on page 32](#).

To update a platform's power policy:

1 Select the platform.

2 Choose **Actions** or right-click the platform.

3 Choose **Operations > Set Power Policy**.

The Console updates the platform's power policy.

To update the power policies of all the platforms in a collection:

Right-click the collection and choose **Collection Operations > Set Power Policy**.

## Synchronizing Clocks

To allow proper management of an AMT platform by the SCS, the AMT platform's system clock must be synchronized with that of the SCS. You can update the Intel AMT device's clock so it is synchronized with the SCS service clock.

To synchronize the Intel AMT device's clock:

- 1 Select the platform.
- 2 Choose **Actions** or right-click the platform.
- 3 Choose **Operations > Synchronize Clock**.

The Console synchronizes the Intel AMT device's clock with the SCS service's clock.

To synchronize the clocks of all the Intel AMT devices in a collection:

Right-click the collection and choose **Collection Operations > Synchronize Clock**.

## Setting Connection Status

You can specify the platform's connection status in the SCS database—**Connected** or **Unconnected**.

To mark the platform's connection status in the SCS database:

- 1 Select the platform.
- 2 Choose **Actions** or right-click the platform.
- 3 Choose **Operations > Set Connection Status**.
- 4 Choose **Connected** or **Not Connected**, depending on how you want to mark the platform's status.

## Authorizing Setup and Configuration

If you chose **AMT requires authorization before performing configuration** in the Network Settings tab of the SCS Service Settings window (see “Network Settings” on page 104), the SCS will not configure any platforms until you expressly authorize it to do so.

To authorize the SCS to configure a platform:

- 1 Select the platform.
- 2 Choose **Actions** or right-click the platform.
- 3 Choose **Authorize AMT**. (This menu choice is visible only if authorization is required and the machine has not yet been configured.)

The SCS now proceeds with configuring the platform.

# 8

---

## Managing SCS Users

This chapter describes how to manage SCS users.

This chapter includes the following sections:

- About Users and Groups
- SCS User Roles
- Viewing Existing Users
- Adding SCS Users
- Deleting SCS Users
- Changing a User's SCS Role

### About Users and Groups

The Users and Groups list defines identities with access to the Intel SCS service and APIs. Each user is assigned a role which defines the permissions allotted to the user. See “SCS User Roles” below for the permissions associated with each role. The console supports assigning a role to a defined group of users.

For example, you can create an SCS Admins group and assign it the Administrator role. Then IT can add users to the group or delete users from it without having to do this from the SCS console.

To improve performance, the SCS maintains a cache of users that access the service. This reduces the number of times that the service needs to access directory services to validate a user. If a user is moved from one group to another, the SCS will continue to use the cache entry to validate the user, and validation may fail as a result. To avoid this failure, flush the cache by restarting IIS.

## SCS User Roles

The operations that an SCS user can perform are dependant on its SCS role. A user can have one of the following roles:

### Enterprise Administrator

The Enterprise Administrator has access to all Intel SCS Console configuration and management screens, fields, and parameters.

### Administrator

The Administrator role has the same permissions as the Enterprise Administrator 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:

- Access Security Keys on the Configuration Service Settings branch.
- View the Status table on the Intel AMT Systems branch.
- View the standard log and the security audit log.
- Access the complete configuration parameters branch.

### Log Viewer

This role allows a user to view the standard log and the security audit log.

### Configuration Client

Users with this role can add platform parameters and request a one-time password (OTP).

The Configuration Client role is required by all platforms executing a client script that communicates directly with the SCS API. This includes the Intel® vPro™ Technology Activator Utility. Add IT-defined groups that contain all computers in each domain that the SCS supports. The SCS does not grant the Configuration Client role to the default Domain Computers Group.

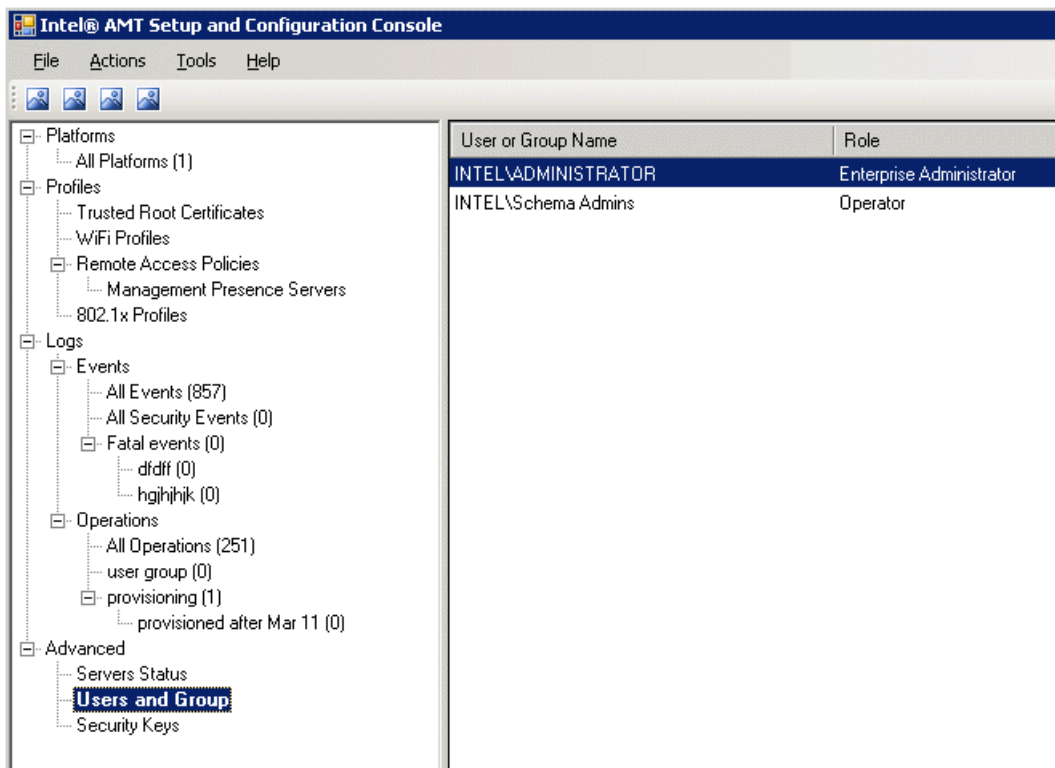
If a user is a member of a group and the group has an assigned SCS role that is different from the user's assigned role, the SCS will grant the user access according to the higher level of permissions. For example, if a user has Enterprise Administrator permissions, and the group has Log Viewer permissions, the user will receive Enterprise Administrator permissions when accessing the SCS. This will also be the case if the group has higher permissions than the user.

## Viewing Existing Users

You can view users that have been given access to the Console.

To view a list of existing users:

In the Console tree, expand the **Advanced** element and click **Users and Groups**. The existing users and groups are displayed. For each user or group, the relevant SCS role is also displayed.





## Adding SCS Users

You can add users to the list of users that can access the Console.

### New User or Group Window

You use this window to add users to the list of users that can access the Console.

To add a user or group:

- 1 Right-click **Users and Groups** and choose **Add**. The New User/Group dialog box is displayed.
- 2 Enter the user's name in the User Name field. Alternatively, click **Select User** to open the standard Windows Select User or Group dialog box, select the user, and click **OK**.
- 3 Choose the user's SCS role in the Role field. For details of the different roles and the operations that each role allows, see "SCS User Roles" on page 90.
- 4 Click **OK** in the New User/Group dialog box. The new user is displayed in the right pane.

User or Group Name	Role
INTEL\ADMINISTRATOR	Enterprise Administrator
INTEL\Schema Admins	Operator
INTEL\John.Smith	Log Viewer

## Deleting SCS Users

You can delete users from the list of users that can access the SCS Console.

---

**Note:** Never remove the SCS service Log On user while the service is running. Removing this user causes the service to fail.

---

To delete a user:

Right-click the user in the right pane and choose **Delete**.

The user is removed from the list.

## Changing a User's SCS Role

You can change the role of an SCS Console user, changing the operations that the user can perform via the Console.

To change a user's role:

- 1 Double-click the user in the right pane, or right-click the user and choose **Edit**.  
The Edit User/Group dialog box is displayed.
- 2 Choose the new role in the Role list and click **OK**. The user's new role is displayed.

# 9

---

## Using USB Drives for TLS-PSK Keys

This chapter describes how to generate TLS-PSK keys, export them to a USB drive, and import them from a file.

### About Using USB Drives for Setup and Configuration

The Factory mode setup process can be simplified by using a USB key containing a file of PID/PPS pairs and replacement passwords, when the BIOS supports this method. This method can be used for one-touch configuration if all the defaults listed below are suitable for an enterprise installation. Even if additional parameters need to be changed, the USB key can install the PID and PPS without the problem of operator error. Use this method also for preparing platforms for future Intel AMT configuration.

---

**Note:** Once you export keys to a USB key, make sure you maintain security so that the key does not fall into the hands of unauthorized people.

---

Before you attempt to create and export TLS-PSK keys, make sure you have a dedicated, bootable USB key with no data on it.

Creating a USB drive with keys involves the following steps:

- 1 Creating a list of PID/PPS/password triplets. For details, see “Configuring Pre-Setup and Configuration Security Keys” on page 96.
- 2 Using the Export function to create a file to write to the USB drive. For details, see “Exporting TLS-PSK Keys to a USB Drive” on page 98.

The SCS automatically formats the drive’s file format to FAT16 and copies the file to the key.

## Configuring Pre-Setup and Configuration Security Keys

Setup and configuration of Intel AMT Release 2.0/2.1/2.5 devices is done using the TLS-PSK (Pre-Shared Key) protocol. Other versions, such as 3.0, can use zero touch configuration but can still be configured using TLS-PSK keys.

The protocol requires a security key installed both in the Intel AMT device and in the SCS database. This pane is used to generate the pre-shared keys and associated parameters.

Each key consists of the following elements:

- **PID:** 8-byte identifier sent in the clear by the Intel AMT device in the “Hello” message.
- **PPS:** 32-byte key.
- **Current MEBx Password:** The Intel AMT platform's administrator's password as programmed in the MEBx by the factory.
- **New MEBx Password:** The password with which the SCS will replace the current password during configuration.

Up to 1024 parameter sets can be exported to a USB key and installed in new Intel AMT devices. Alternately, an OEM may ship platforms with PID/PPS pairs and a default password already installed. In this case, the file from the OEM must be imported into the SCS database. The third option is entering the PID and PPS manually. (This option is outside the scope of this book.)

To view the security keys that will be accepted by the SCS:

In the Console tree, expand the **Advanced** element and click **TLS-PSK Security Keys**. The current security keys are displayed.

PID	PPS	Current MEBx Password	New MEBx Password
4444-4444	0000-0000-0000-0000-0000-0...	Admin@98	Admin@98
NGQA-D4VX	93YH-HGHZ-RPLM-V9AS-0...	Admin@98	Admin@98
M7PL-DK08	12NX-665H-P9ZB-2N40-009...	Admin@98	Admin@98
3D0P-6INK	4N0Y-3S51-F66Y-RUFL-K50...	Admin@98	Admin@98
W497-2YCP	4HLK-EJEW-XQMS-H3B9-5Y...	Admin@98	Admin@98
Y7GD-SMJD	0DBX-NS4X-B1PF-FGM2-8V...	Admin@98	Admin@98
E310-TS4Z	TJYV-V2IT-HV5V-Q2OU-JY7...	Admin@98	Admin@98
DCG6-FEM8	BMK2-E7DC-XLIL-QA2J-H7X...	Admin@98	Admin@98
YW64-11LO	MEF0-FCIU-YGA9-98ZN-TGZ...	Admin@98	Admin@98
DCXQ-ZKN7	ZKFJ-GWVS-ARE0-0INJ-550...	Admin@98	Admin@98
AIYQ-TS6P	Y2ES-IGM5-1TNV-DSB1-D7...	Admin@98	Admin@98

To refresh the list of security keys:

Right-click **Security Keys** and choose **Refresh List of Keys**.

## Creating TLS-PSK Security Keys

To create TLS-PSK security keys, do the following:

- 1 In the Advanced element, right-click **TLS-PSK Configuration Keys** and choose **Add Security Keys**. The Security Key Settings window opens.
- 2 Specify the following information where applicable:
  - **Number of keys to store:** The number of keys that you want to create (up to 1024 keys)
  - **Manufacturing default MEBx password:** the MEBx password that was entered in the firmware by the manufacturer.
  - **New MEBx Password:** Choose the type of new MEBx password:
    - **Randomize password:** Choosing this creates a different, random password for each key.
    - **Fixed Password:** To use the same password with all the keys, choose this and enter the password that you want to use.

**3** Click **OK**.

The Intel SCS creates a list of Security Keys. See the MEBx Settings pane to configure the number of keys generated. Each record consists of an 8 byte PID, a 32 byte PPS and the administrator's password. To view the keys, expand the **Advanced** element and click **TLS-PSK Security Keys**.

## Exporting TLS-PSK Keys to a USB Drive

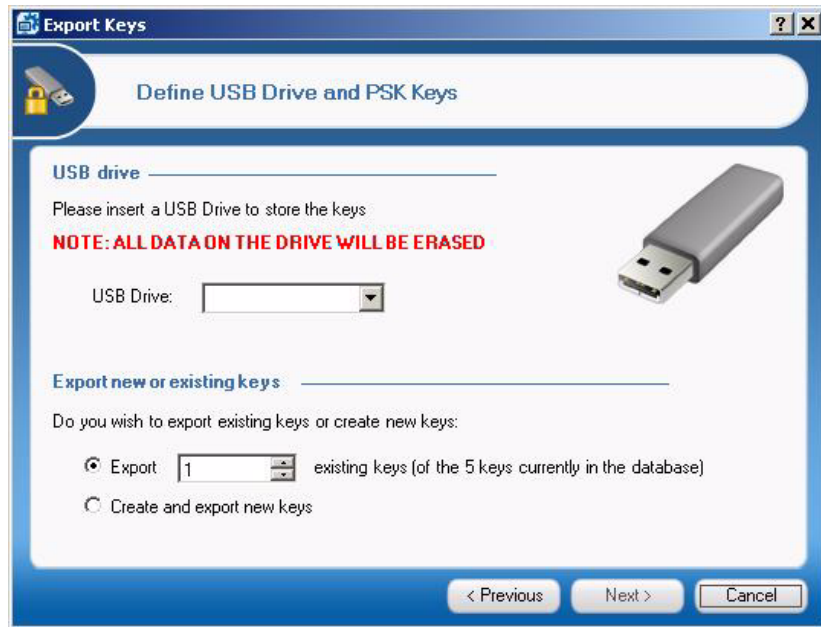
You can export TLS-PSK security keys to a file on a USB drive in the format expected by an Intel AMT platform's BIOS.

To export the list of keys to a USB drive:

- 1** Attach a USB drive to a USB port on the server on which the Console is running.
- 2** In the Advanced element, right-click **TLS-PSK Configuration Keys** and choose **Export Keys to USB Drive**.

The Export Keys wizard opens and displays a welcome screen.

- 3 Click **Next**. The Define USB Drive and PSK Keys window is displayed.

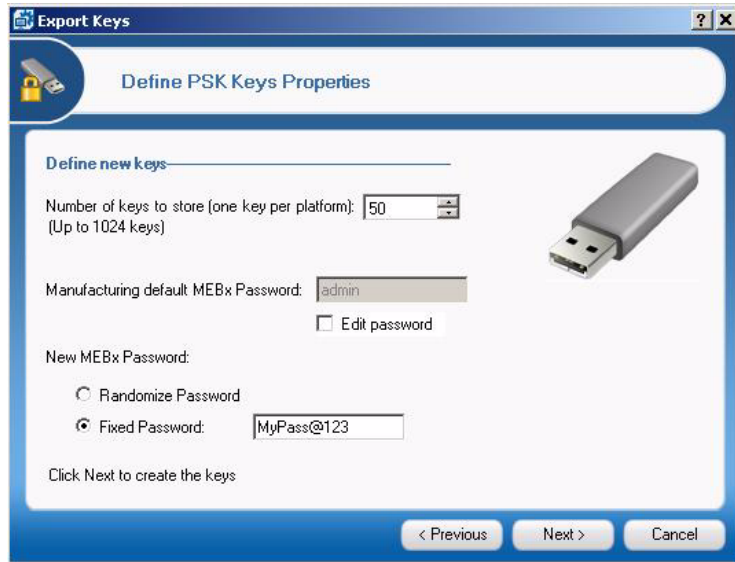


### Export Key Wizard

You use the Export Key wizard to export a list of TLS-PSK keys to a USB drive.

- 1 In the **USB Drive** list, choose the drive to which you want to export the keys.
- 2 To export existing keys, select the **Export** option. Then specify the number of keys that you want to store on the drive (up to 1024 keys). Click **Next** to export the keys and finish this procedure. To create and export new keys, go to step 3.

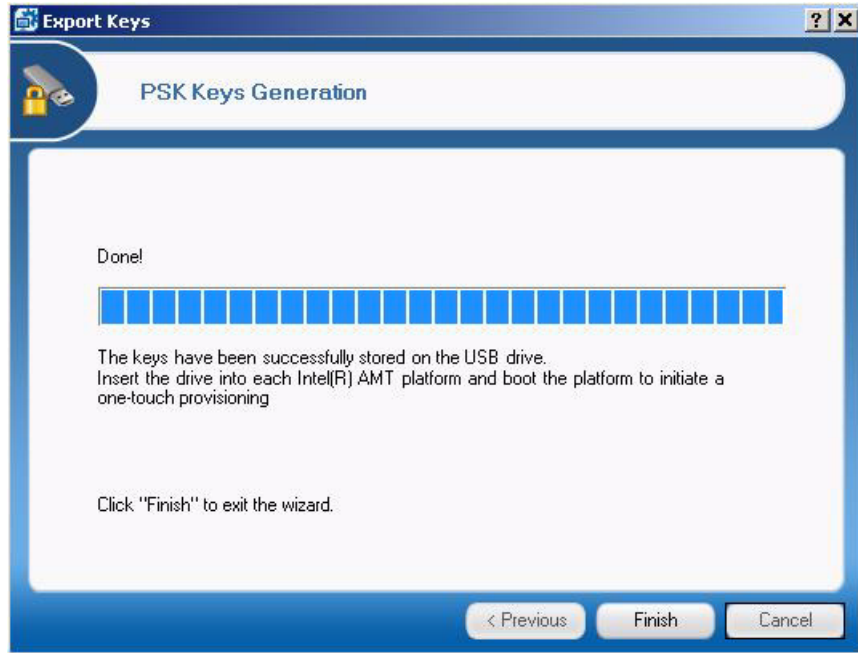
- 3 To create and export new keys, select the **Create and Export new keys** option. The Define PSK Keys window is displayed.



- 4 In the **Number of keys to store** field, enter a value of up to 1024 keys.
- 5 In the **Manufacturing default MEBx Password** field, enter the MEBx password that was entered in the firmware by the manufacturer. Check the box next to **Edit password** to change the password.
- 6 To use the same password with all the keys, select **Fixed Password** and enter the password that you want to use.
- 7 To generate a different, random password for each key, select **Randomize Password**.
- 8 Click **Next**.



- 9 Confirm that you want to format the drive and proceed with exporting the keys. The wizard displays a progress bar.



- 10 When all the keys have been exported to the USB drive, click **Finish** to exit the wizard.

## Importing Keys

You can import keys into SCS from a file. This function is useful when you need to add a file of keys from an OEM to the SCS database. You can import keys from a file created in accordance with the OEM's instructions for manufacturing Intel AMT systems.

To import a file of keys:

- 1 Attach a USB drive to a USB port on the server on which the Console is running.
- 2 In the Advanced element, right-click **TLS-PSK Configuration Keys** and choose **Import Keys from File**. A browse dialog box is displayed.
- 3 Locate the key file (**setup.bin**) in the USB drive and click **Open**.

The Console imports the keys and displays them when you click **TLS-PSK Configuration Keys** in the **Advanced** tree element.

# 10

---

## Viewing and Configuring SCS Services

This chapter describes how to view and configure settings related to the SCS services.

This chapter includes the following sections:

- Network Settings
- Maintenance Policies
- Log Settings
- AMT Configuration Parameters
- Performance Settings

### About SCS Service Settings

You view and change SCS service settings via the SCS Service Settings window.

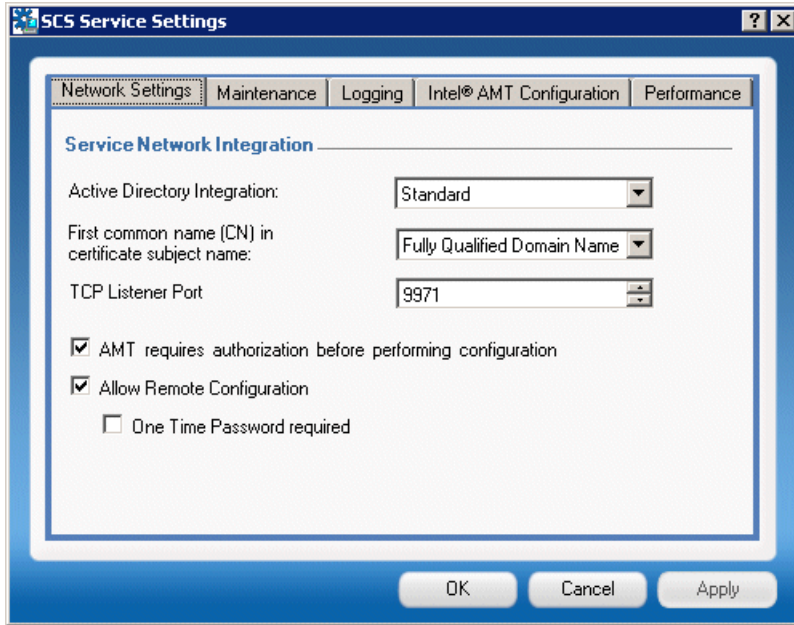
To access the service settings:

- 1 Click **Tools > Service Settings**. The Service Settings window opens.
- 2 Click the relevant tab to access the settings that you want to view or modify:

See the following sections for a description of each tab.

## Network Settings

You use the Network Settings tab to view or modify the SCS service's network settings.



### SCS Service Settings Window

- **TCP Listener Port:** Each instance of Intel SCS listens for “Hello” messages from Intel AMT devices on a defined TCP port. Enter the TCP port used for listening. The default port is 9971.
- **First common name (CN) in certificate subject name:** In this list, specify the format that the AMT machine expects for the first CN in a certificate. This can be one of the following:
  - **Fully-Qualified Domain Name:** FQDN of the Intel AMT device
  - **Host Name:** Host name of the platform (available if integration with Active Directory is enabled)
  - **SAM Account name:** Active Directory account name for the AMT object (available if integration with Active Directory is enabled)

- **Active Directory Integration:** Enables the use of Kerberos authentication and the Active Directory users list. Active Directory Integration must be enabled to configure an Intel AMT device for wired 802.1x, or for wireless when the wireless profile uses 802.1x for authentication.
  - **None:** Do not integrate with Active Directory.
  - **Schema Extension:** Integrate with Active Directory and cause the SCS server to add AMT objects to Active Directory. Intel recommends using this method.
  - **Standard:** Integrate with Active Directory without extending the schema.
- **AMT requires authorization before performing configuration:** When the SCS receives a "Hello" message from an Intel AMT device, setup and configuration will proceed automatically, unless this checkbox is selected. Selecting this checkbox requires the Console operator to authorize setup and configuration of the specific platform via the **Authorize AMT** function. See “Authorizing Setup and Configuration” on page 88.
- **Allow Remote Configuration:** Intel AMT Releases 2.2, 2.6 and 3.0 and later releases 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 checkbox enables the SCS to accept self-signed certificates from Intel AMT devices.
  - **One Time Password Required:** Selecting this checkbox adds an additional security feature to the Remote Configuration process. An enterprise policy may require a one-time password (OTP) exchange between the SCS and the Intel AMT device requesting setup. If you check this box, the SCS will perform configuration only after receiving and verifying the OTP from the platform. **Note:** So-called "Bare-Metal" platforms are certain platforms that contain Intel AMT Release 3.0 or higher that are configured by the manufacturer to start sending Remote Configuration "Hello" messages as soon as they are connected to the network. Bare Metal platforms do not support one-time passwords. Therefore, selecting the One time Password Required option prevents configuring bare-metal platforms.

## Maintenance Policies

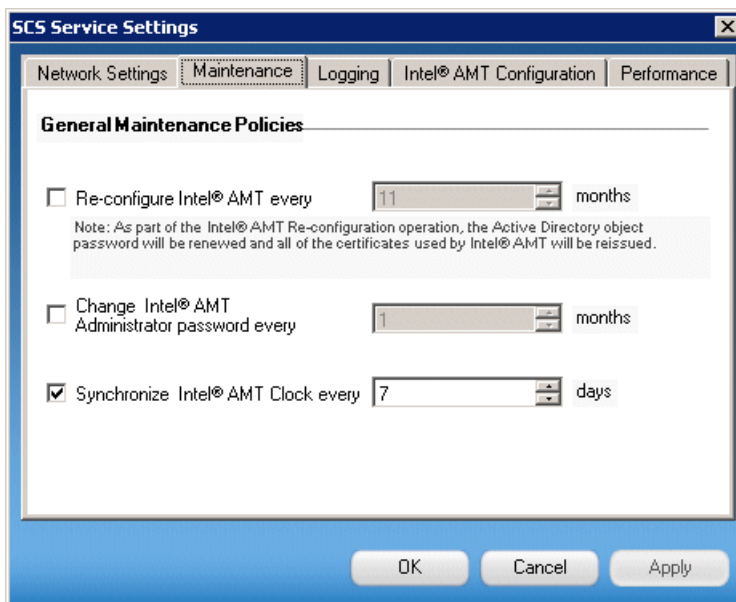
The Maintenance tab defines actions that the SCS will perform periodically on all configured Intel AMT devices. The items enabled with a checkbox can be used to implement a specific site security policy.

The SCS will queue a request for an Intel AMT device only if there is no other request pending for that device. Since maintenance actions apply to all devices, the SCS does not perform a scheduled action on devices already waiting for some other action to occur. This will not be reported as an error.

---

**Note:** If TLS is not enabled, maintenance messages to the Intel AMT devices are sent in the clear, without encryption. It is recommended that in non-TLS environments, passwords for the AMT objects in Active Directory should be configured as "Password Never Expires", and that the maintenance function should be used only to synchronize the Intel AMT clock.

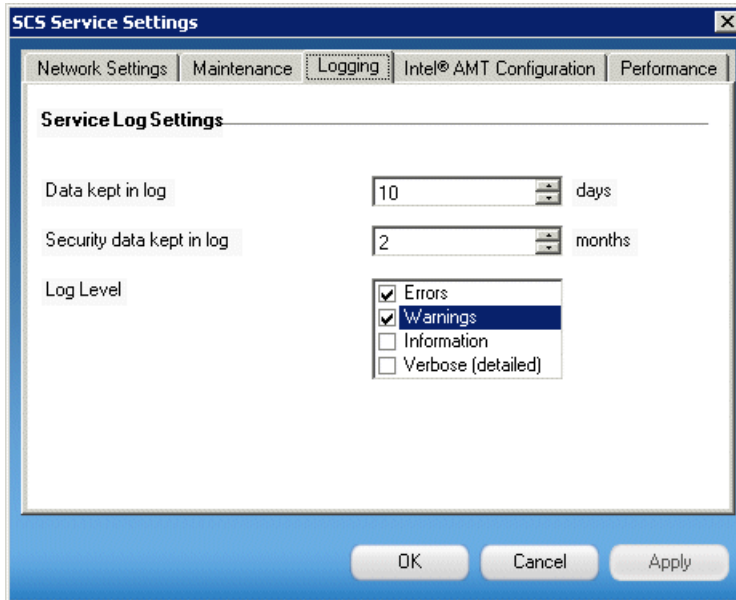
---



- **Reconfigure Intel AMT every:** Perform reconfiguration periodically with the current values in the associated profile without user intervention. This ensures that all the Intel AMT devices have the latest profile information.
- **Change Intel AMT Administrator password every:** The administrative user has access to all functions of the Intel AMT device. Only the 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 General section of the definition of the profile associated with each Intel AMT device (see “Creating a Profile” on page 29). Normally, this maintenance function is used only with the random password option.
- **Synchronize Intel AMT clock every:** This option synchronizes the clock in each Intel AMT device to the clock on the 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.

## Log Settings

The Logging tab allows you to specify log settings.

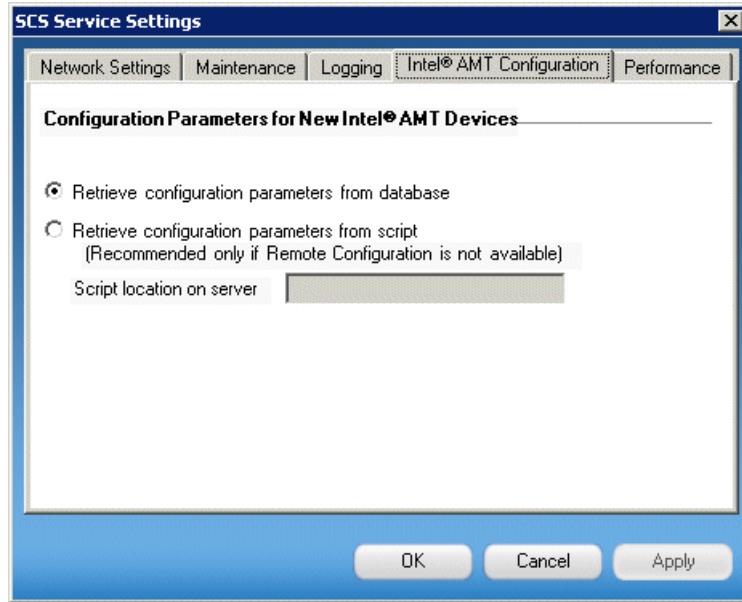


- **Data kept in log:** The number of days the log messages are stored before they are deleted.
- **Security data kept in log:** The number of months the security messages are stored in the log before they are deleted.
- **Log level:** The level of detail of the information stored in the log. Note that the more detail recorded, the more system resources and bandwidth must be allocated..
  - **Errors:**
  - **Warnings:**
  - **Information:**
  - **Verbose (detailed):** Useful for advanced system debugging



## AMT Configuration Parameters

You use this tab to specify how the SCS should acquire the necessary information defining the Intel AMT device properties.



- **Retrieve configuration parameters from database:** The SCS searches the Configuration parameters table stored in the SCS database for the properties of each Intel AMT platform.

- **Retrieve configuration parameters from script:**

---

**Note:** Recommended only if the Activator is not available.

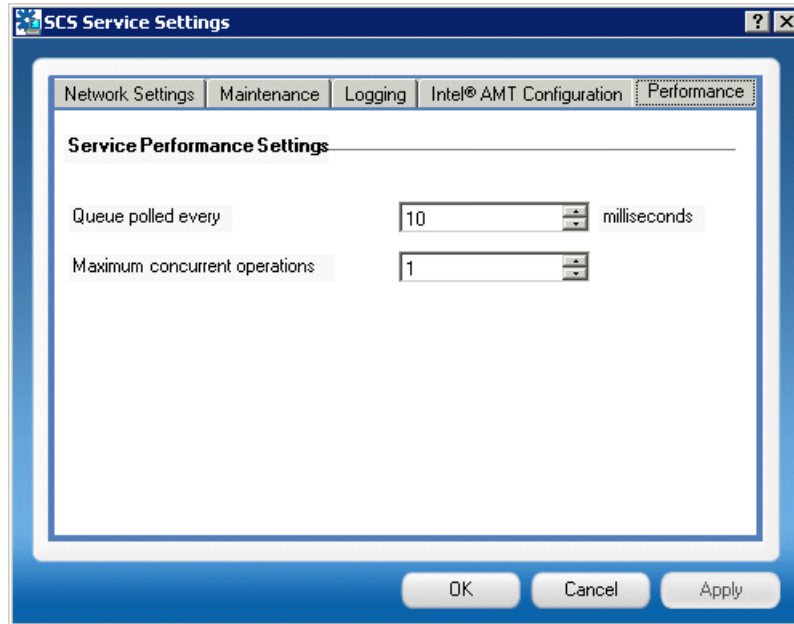
---

When this option is selected, the SCS first searches the Configuration parameters table for a matching entry, based on the UUID in the "Hello" message. If there is no matching entry, the SCS determines the properties by invoking a script written by the controlling enterprise and which either refers to an independent database or file or requests the identifying information from the host platform. After the script returns the required information, the SCS stores the information in the Configuration data table. See [Using a Script to Import Intel AMT Configuration Properties](#).

- **Script location on server:** Enter the path to the location of the script on the platform where the SCS executes. If there is more than one instance of the service running in the domain, the script must be in the same location on all platforms running the service. (e.g., C:\program files\intel\AMTConfserver\scripts\). **Warning:** If the script is not in the location specified here, the SCS will not complete setup for any Intel AMT devices.

## Performance Settings

You use this tab to specify parameters that can affect the SCS service's performance.



- **Queue polled every ... milliseconds:** Determines how frequently the Intel SCS checks the queue in the database for new tasks.
- **Maximum concurrent operations:** Determines the maximum number of SCS operations that can be performed concurrently by each SCS service (for example, configuring or unconfiguring an Intel AMT platform, synchronizing clocks, and so on). This value can be adjusted to optimize the service's performance, depending on the number of CPUs and the memory size.



# 11

---

## Viewing Log files

This chapter describes the log files that the Intel SCS generates.

The chapter includes the following sections:

- About the Log Files
- Using the Event Logs
- Using the Operations Log
- Creating View Collections
- Creating View Subcollections
- Exporting Log Files

### About the Log Files

The SCS generates log files that include information on SCS events and operations. You can create filters that allow you to display specific types of log messages.

## Using the Event Logs

The event log provides information about all the events that take place in the SCS. There are the following types of event logs:

- All Events log
- Security Events log

### All Events Log

This log displays system-wide actions. This includes actions that succeeded and actions that failed. In particular, this log highlights failed actions. The log messages can be filtered by date, by message type, and by severity. The Log Level setting on the General Settings screen determines the number and level of messages displayed in the log. See the SCS Troubleshooting Guide for a description of these messages and the action to take to correct a detected error.

To view the All Events log:

Expand the **Events** element and click **All Events**. Details for the selected record in the log are displayed at the bottom of the window.

- [-] Platforms
  - All Platforms (1)
- [-] Profiles
  - Trusted Root Certificates
  - WiFi Profiles
  - [-] Remote Access Policies
    - Management Presence Servers
  - 802.1x Profiles
- [-] Logs
  - [-] Events
    - All Events (857)**
    - All Security Events (0)
  - [-] Operations
    - All Operations (251)
- [-] Advanced
  - Servers Status
  - Users and Group
  - Security Keys

Severity	Description	Date and Time	FQDN
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:52:15 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:50:55 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:49:35 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:48:15 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:46:55 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:45:34 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:44:14 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:42:53 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:41:33 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:40:13 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:38:52 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:37:32 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:36:12 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:34:52 PM	
SeverityError	Error Configuring Intel AMT de...	3/11/2008 3:33:31 PM	

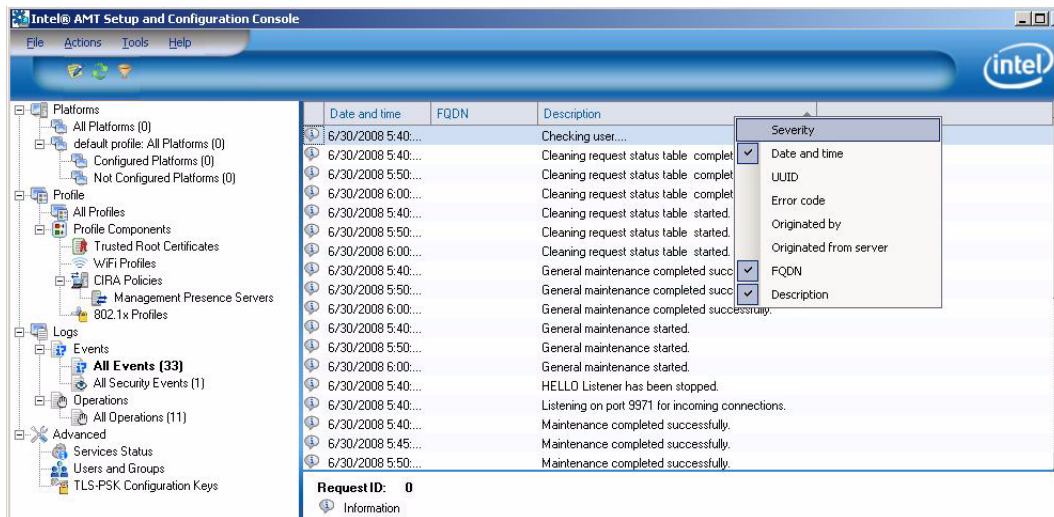
The Console displays the following information about each event:

- Severity

- Description
- Date and Time
- FQDN

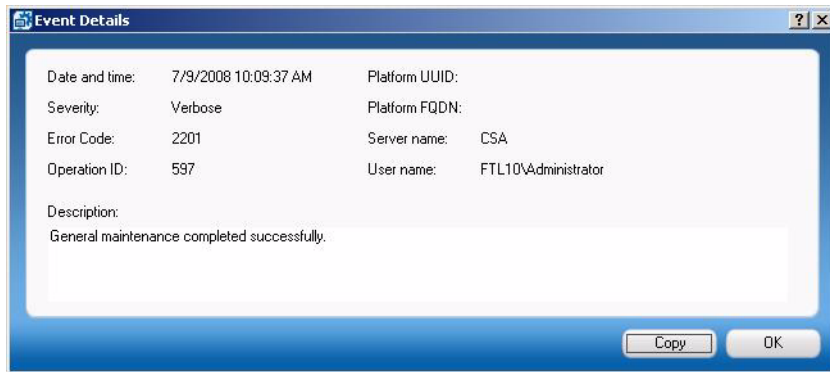
You can add or remove additional information fields by right-clicking the bar containing the field descriptions. Additional fields include:

- UUID
- Operation ID
- Originated by
- Originated from server
- Error code
- Request ID



To view detailed information about a specific event:

Double-click the event. The Console displays the Event Details window.



## Event Details Window

In addition to the information displayed in the main Console window, the Event Details window also displays the following:

- Platform UUID
- Error code
- Operation ID
- Server name: Name of the server running the Intel SCS service
- User name: Name of the user account running the Intel SCS service

When you select a specific event, all of the details are displayed at the bottom of the console.



## Security Events Log

This log displays potential breaches in security, such as unauthorized attempts to log-in and unauthorized attempts to perform the reconfiguration function on all Intel AMT devices. The security log also registers valid events that have security impact, such as user log-ins. The SCS logs the following events in the security log:

	Event
Error	Cannot contact CA server - Process delayed.
Error	Certificate cannot be issued - Process interrupted.
Error	Cannot request CA - Process interrupted.
Error	Working without CA - Process interrupted.
Error	Invalid network TLS authentication value
Error	Fail to delete Certificate
Error	User is not authorized
Error	Failed to remove profile.
Error	Unexpected exception when requesting certificate: - Process interrupted.
Error	Cannot contact unconfigured Intel AMT device without PID/PPS.
Error	Cannot obtain connection to Intel AMT device on nn.
Information	Certificate request already under submission - Process delayed.
Information	Set Certificate Template
Information	User logged in.
Information	Modify user account nn.
Information	Set EACL.
Information	Set FPACL.
Information	Set general parameters for profile.
Information	Adding TLS server certificate.

To view the Security Events log:

Expand the **Events** element and click **All Security Events**.

The Console displays the following information about each security event:

- Severity
- Description
- Date and Time
- FQDN

You can add or remove additional information fields by right-clicking the bar containing the field descriptions. Additional fields include:

- Platform UUID
- Error code
- Request ID
- Server name: Name of the server running the Intel SCS service
- User name: Name of the user account running the Intel SCS service

To view detailed information about a specific event:

Double-click the event. The Console displays the Event Details window.

In addition to the information displayed in the main Console window, the Event Details window also displays the following:

- Platform UUID
- Error code
- Request ID
- Server name: Name of the server running the Intel SCS service
- User name: Name of the user account running the Intel SCS service

## Using the Operations Log

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.

The SCS checks its queues every five minutes to see if it is time to perform a scheduled maintenance task. The SCS records this in the Actions Status log as a maintenance task, even if no other activity was performed. Each of the maintenance events is noted as a CleanLog and ClearRequestStatus event. Note that an actual CleanLog event occurs only once every 24 hours.

To view the Operations log:

- 1 In the Logs element, expand **Operations** and click **All Operations**.

Status	Operation	Date and Time	Platform UUID
Succeeded	Maintenance	3/10/2008 3:52:23 PM	
Succeeded	Maintenance	3/10/2008 3:47:22 PM	
Delayed	ReProvision	3/11/2008 3:46:55 PM	03020100-0504-0706-0809-C
Succeeded	Maintenance	3/10/2008 3:42:23 PM	
Succeeded	Maintenance	3/10/2008 3:37:22 PM	
Succeeded	Maintenance	3/10/2008 3:32:22 PM	
Succeeded	Maintenance	3/10/2008 3:27:23 PM	
Succeeded	Maintenance	3/10/2008 3:22:22 PM	
Succeeded	Provision	3/10/2008 2:24:55 PM	03020100-0504-0706-0809-C
Succeeded	Maintenance	3/10/2008 3:12:22 PM	
Succeeded	Maintenance	3/10/2008 3:07:22 PM	
Succeeded	Maintenance	3/10/2008 3:02:23 PM	
Succeeded	Maintenance	3/10/2008 2:57:22 PM	
Succeeded	Maintenance	3/10/2008 2:52:22 PM	
Succeeded	Maintenance	3/10/2008 2:47:22 PM	
Succeeded	Maintenance	3/10/2008 2:42:22 PM	
Succeeded	Maintenance	3/10/2008 2:37:23 PM	
Succeeded	Maintenance	3/10/2008 2:32:23 PM	
Succeeded	Maintenance	3/10/2008 2:27:23 PM	
Succeeded	Maintenance	3/10/2008 2:22:23 PM	

SCS service is stopped Connected to server:https://DC.intel.com/AMTSCS

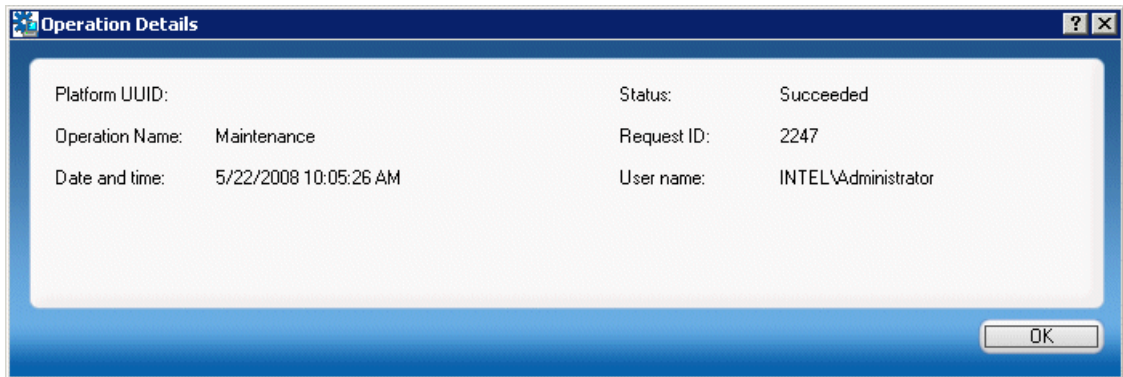
The Console displays the following information about each operation:

- ID

- Status
- Operation
- Date and Time
- User
- Platform UUID

To view detailed information about a specific operation:

Double-click the operation. The Console displays the Operation Details window.



## Operation Details Window

The Operation Details window displays the following:

- Platform UUID
- Status
- Operation name
- Request ID
- Date and time
- User name: Name of the user account running the Intel SCS service

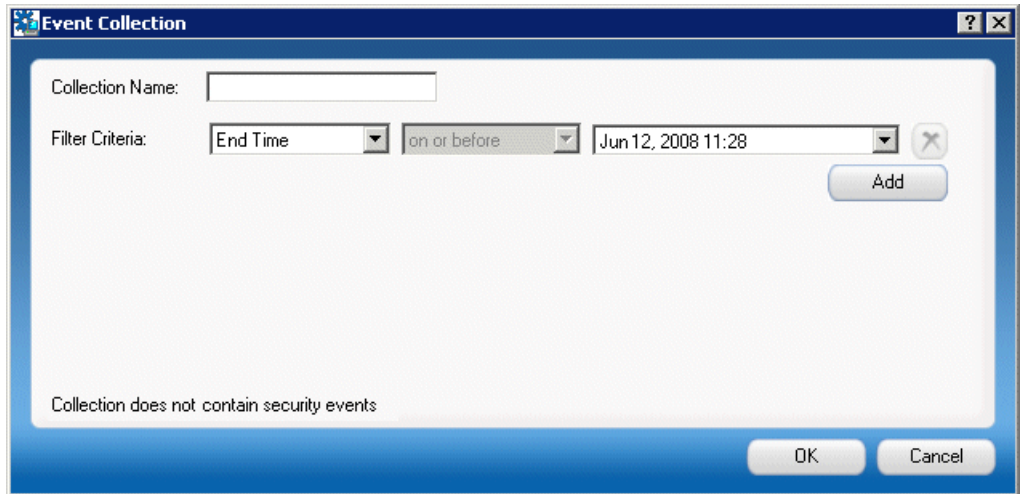
## Creating View Collections

You can create a view to display a subset of the messages in the log filters. This view is known as a *collection*. You can create event collections and operation collections.

To create an event collection:

- 1 In the Console tree, right-click the **Events** element and choose **Create Event Collection**.

The Event Collection window is displayed.



### Event Collection Window

You use the Event Collection window to create an event collection, which is a view showing a subset of the messages in the log filters.

- 1 In the left-most field, choose the filter type and the appropriate values in the remaining fields. The filter type defines the values in the remaining fields.

The following table describes the available choices for each type of filter:

Filter Type	Operator	Operand	Comments	
Start Time		A date chosen from the calendar that appears when you click the field's down-arrow		
End Time		A date chosen from the calendar that appears when you click the field's down-arrow		
Severity	<ul style="list-style-type: none"> <li>• is or higher than</li> </ul>	<ul style="list-style-type: none"> <li>• Fatal</li> <li>• SeverityError</li> <li>• Warning</li> <li>• Information</li> <li>• Debug</li> </ul>		
Description	<ul style="list-style-type: none"> <li>• is</li> <li>• contains</li> <li>• starts with</li> <li>• ends with</li> </ul>	<ul style="list-style-type: none"> <li>• Any string comprising part or all of a host name</li> </ul>		
Request ID	<ul style="list-style-type: none"> <li>• is</li> </ul>	Any string comprising part or all of a request ID		

Filter Type	Operator	Operand	Comments	
Message ID	• is	Any string comprising part or all of a message ID		
Platform UUID	is	A string comprising part or all of a UUID		

- 2 Enter a name for the collection in the Collection Name field.
- 3 To add another filter condition, click **Add** and enter the relevant values. Continue adding filter conditions until the filter is complete.

At the bottom of the window, a note indicates whether the collection contains security events.

- 4 Click **OK**.

The new event filter appears as a sub-element of the Events element.

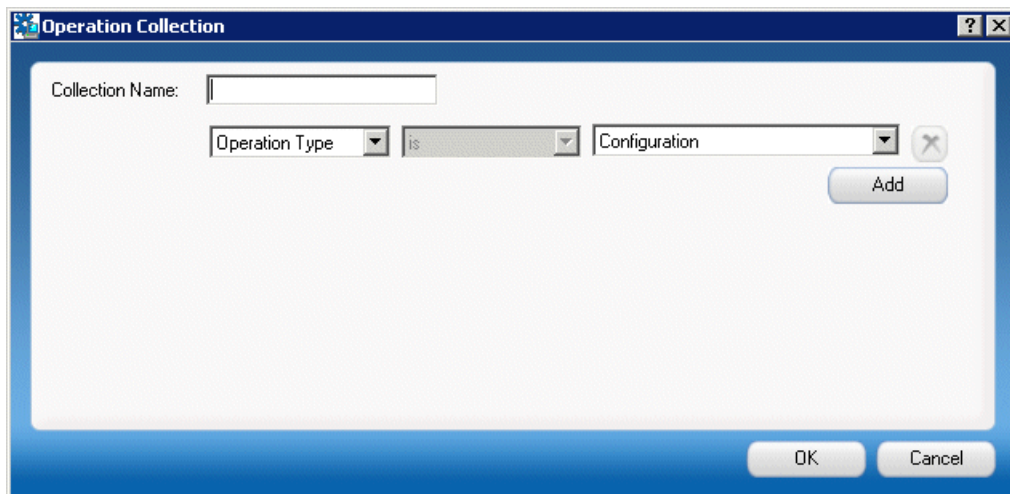
To display all the events that meet the filter criteria:

Click the event filter. The events are displayed in the right pane.

To create an operation collection:

- 1 In the Console tree, right-click the **Operations** element and choose **Create Operation Collection**.

The Operation Collection window is displayed.



## Operation Collection Window

You use the Operation Collection window to create an operation collection, which is a view showing a subset of the operations written to the log.



- 1 In the left-most field, choose the filter type and the appropriate values in the remaining fields. The filter type defines the values in the remaining fields.

The following table describes the available choices for each type of filter:

	Operator	Operand	Comments
Operation Type	is	<ul style="list-style-type: none"> <li>• Configuration</li> <li>• Reapply configuration</li> <li>• Reset of configuration to factory defaults</li> <li>• Partial configuration reset</li> <li>• UpdateAmtAcl</li> <li>• ReissueDigitalCertificate</li> <li>• SetAmtPowerPolicy</li> <li>• UpdateAmtCrl</li> </ul>	
Start Time		A date chosen from the calendar that appears when you click the field's down-arrow	
End Time		A date chosen from the calendar that appears when you click the field's down-arrow	
Status	is	<ul style="list-style-type: none"> <li>• InProgress</li> <li>• InQueue</li> <li>• Waiting</li> <li>• Delayed</li> <li>• Succeeded</li> <li>• Failed</li> </ul>	
Request ID	is	Any string comprising part or all of a request ID	
Username	is	Any string comprising part or all of a user name	

- 2 Enter a name for the collection in the Collection Name field.
- 3 To add another filter condition, click **Add** and enter the relevant values. Continue adding filter conditions until the filter is complete.
- 4 Click **OK**.

The new operation filter appears as a sub-element of the Operations element.

To display all the operations that meet the filter criteria:

Click the operation filter. The operations are displayed in the right pane.

## Creating View Subcollections

After you create a view collection, you can create a subcollection to display a subset of the events or operations defined in the collection. For example, after defining a collection of all the configuration operations that occurred, you can define a subcollection that includes only the configuration operations that occurred after a certain time.

To create an event or operation subcollection:

- 1 In the Console tree, right-click the event collection or operation and choose **Create Event Subcollection** or **Create Event Subcollection**, respectively. The window that opens allows you to add filters to the existing collection. Note that the window already displays the values that were defined for the collection and an additional row for you to edit.
- 2 Complete creating the subcollection in the same way as you would create a collection. For details of creating collections, see “Creating View Collections” on page 121.

The subcollection appears in the tree as a sub-element of the collection.

To display the events or operations in the subcollection:

Click the subcollection in the Console tree. The events or operations are displayed in the right pane.

## Exporting Log Files

You can export the messages in the event log collections and subcollections. The Console creates a .csv file containing the log messages.

To export the event log messages:

- 1 Right-click the event log collection or subcollection, or select the collection or subcollection.
- 2 **Choose Export Logs.** A browse window opens. The window already contains a name for the .csv file that will be created by the exporting.
- 3 Specify the location where you want to store the .csv file and click **Save**. The Console saves the file in the specified location.



# 12

---

## Localization

This chapter provides information on using the SCS Console on computers with non-English language operating systems.

This chapter includes the following section:

- Internationalization of SCS Messages

### Internationalization of SCS Messages

The SCS was designed to support internationalization of the user interface. The service and the associated API display all status, warning, and error messages based on a single file. The application executables retrieve a message based on a message number and the current language on the platform where the application executes. If the message file supports the current language, then the file will return the message in the proper language. If the file does not support the current language, it will return the message in English. See the document *Internationalization of SCS Messages.doc* for the steps required to add an additional language to the message file.



# Part IV

---

## Appendixes

This part contains the following chapters:

- Remote Configuration
- CRL XML Format
- Using a Script to Import Intel AMT Configuration Properties





# A

---

## Remote Configuration

This chapter provides information on using the remote configuration feature.

The chapter includes the following sections:

- About Remote Configuration
- Remote Configuration Flow
- Intel AMT Release 3.0 Additional Features
- Remote Configuration Certificate – Differences between Releases
- Intel® vPro™ Technology Activator Utility

## About Remote Configuration

Remote Configuration is a feature added with Intel AMT Releases 2.2, 2.6, and 3.0 and later releases. It eliminates the need for IT personnel to manually install a PID/PPS pair to enable setup. The Remote Configuration process depends on several Intel AMT enhancements:

### Embedded hashed root certificates

The Intel AMT device contains one or more root certificate hashes from worldwide SSL certificate providers in the firmware image. As part of the “Hello” message, the Intel AMT device sends all of the hashes to the SCS. When the SCS authenticates to the Intel AMT device, it must do so with a certificate compatible with one of the hashed root certificates.

### Self-signed certificate

The Intel AMT device produces a self-signed certificate that it uses to authenticate to the SCS. The SCS must be configured to accept such a certificate.

### One-time password (OTP)

Security policy may require use of a one-time password to improve security. The Intel® vPro™ Technology Activator Utility running on the local host requests the OTP from the SCS and sends it to the Intel AMT device. The SCS saves the OTP in the database entry associated with the specific Intel AMT device, and uses it to validate the connection to the device.

### Limited network access

The network interface opens for a limited period of time to send “Hello” messages and to complete the setup and configuration process. After 24 hours, the interface will close if the setup and configuration time was not extended by a network command from the SCS.

## Remote Configuration Flow

### Initial Conditions

Before Remote Configuration begins, the following initial conditions must be met:

- The Intel AMT device is configured to receive its IP address from a DHCP server. The DHCP server supports option 15 and will return the local domain suffix.
- The Intel AMT device is pre-programmed with at least one active root certificate hash.
- For the delayed installation sequence described below (“delayed” meaning that the Intel AMT device was not setup immediately upon being connected to the network; see “Bare Metal Setup and Configuration” on page 145), the Intel® vPro™ Technology Activator Utility must be executed on the host platform.
- The SCS is registered with a DNS server accessible to the Intel AMT device with the name “Provisionserver” (or the name defined by the OEM) and is in either the same domain as the device or it is in a domain with the same suffix.
- The SCS has a certificate with Server Authentication Certificate usage with the appropriate **OID** or **OU** that traces to a CA which has a root certificate hash stored in the Intel AMT device.

The OID in the Extended Key Usage field must have an Intel setup extension:

1.3.6.1.5.5.7.3.1,2.16.840.1.113741.1.2.3

**or**

the **OU** value in the **Subject** field must be “**Intel(R) Client Setup Certificate**”.

The Subject CN must match the domain suffix of the Intel AMT platform (see “Remote Configuration Certificate – Differences between Releases” on page 146).

- The SCS is configured to allow remote configuration. The checkbox on the Console Service Settings/General screen for **Allow configuration with certificate-based configuration** must be checked. **One-time password required** should be checked if one-time passwords will be used.

## Acquiring and Configuring a Certificate that Supports Remote Configuration

Contact one of the vendors whose root certificate hashes are built into the Intel AMT firmware. A list of the hashes should be provided by the platform vendor. Go to the vendor's website and purchase an "SSL certificate".

For example, the following link to Verisign's\* site shows how to purchase an appropriate certificate:

<http://www.verisign.com/ssl/buy-ssl-certificates/index.html>

The site documents in detail the steps required to request, enroll, install and move an SSL certificate. The following settings are required for the certificate to be compatible for Remote Configuration use:

- The OU or the OID must match the values defined in [“Initial Conditions” on page 135](#) (the OU is the usual value entered when purchasing a certificate commercially).
- The CN must match the Intel AMT platform domain suffix (see “Remote Configuration Certificate – Differences between Releases” on page 146).
- The keys should be exportable to support IT key backup policies.
- The request type should be PKCS10.

After completion, export the acquired certificate in p7c format.

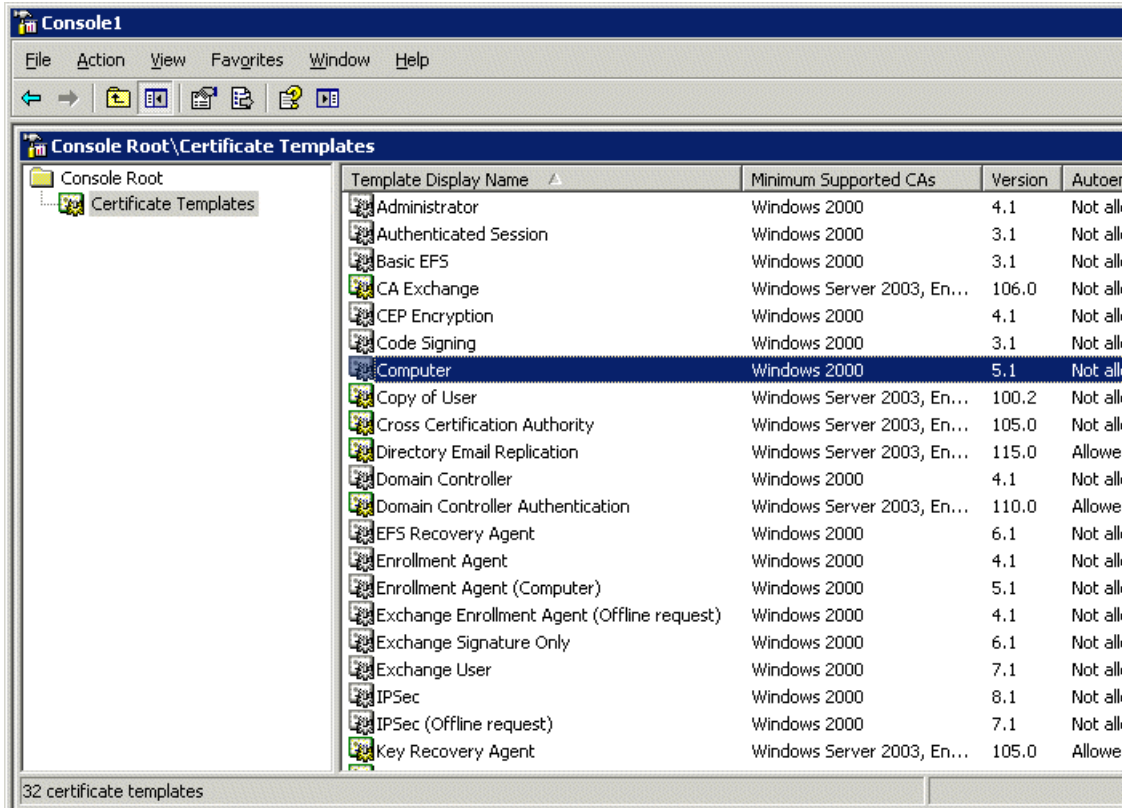
## Creating and Installing Your Own Certificate

This section describes how you can install your own certificate to allow remote configuration.

To install your certificate:

- 1 Enter **mmc** in a Command window.
- 2 Choose **File > Add/Remove Snap-in**.
- 3 Click **Add** and select **Certificate Templates**.
- 4 Click **Close** in the Add Standalone Snap-in window, and then click **OK** in the Add/Remove Snap-in window. The Certificate Templates element is added to the left pane.

- 5 In the Console Root window, double-click **Certificate Templates**.



- 6 In the right-pane, right-click the **Computer** template and choose **Duplicate Template**. The Properties of New Template window opens.
- 7 In the Template Display Name field, enter a name for the template.
- 8 Click the **Extensions** tab, click Application Policies and click **Edit**. The Edit Application Policies Extension window opens.
- 9 Click **Add**. The Add Application Policy window opens.
- 10 Click **New**. The New Application Policy window opens.
- 11 Enter a policy name, and in the Object Identifier field enter the following OID for Remote Configuration: **2.16.840.1.113741.1.2.3**

- 12 Click **OK** to return to the Add Application Policy window, click **OK** to return to the Edit Application Policies Extension window, and click **OK** to return to the Properties of New Template window.
- 13 Click the **Subject Name** tab and choose **Supply in the request**.
- 14 Click the **Request Handling** tab and check the **Allow private key to be exported** box.
- 15 Click **OK**.
- 16 Open the Certificate Authority and click **Certificate Templates**.
- 17 Right-click in the right pane and choose **New > Certificate Template to Issue**.
- 18 In the Enable Certificate Templates window, choose the template that you just created and click **OK**. The template now appears in the right pane with the other certificate templates.
- 19 On the SCS machine, open Internet Explorer and connect to Certificate Services for the Root CA by browsing to **http://CA\_FQDN/certsrv**.
- 20 Request a certificate
- 21 Advanced certificate request
- 22 Create and submit a request to this CA.
- 23 In the Certificate Template drop-down list, choose the Remote Config Template (the certificate template that you created).
- 24 In the Identifying Information for Offline Template section, enter the domain name where the certificate will be used (SCS machine domain suffix or FQDN) in the **Name** field.
- 25 Leave all the other default values and click **Submit**.
- 26 Install the certificate in the SCS application user's certificate store.
- 27 In the Console, choose **Tools > Service Settings**. In the Network Settings tab, check the **Allow Remote Configuration** box and click **OK**.

## Creating a Multipurpose Certificate Template

Intel SCS 5.0 includes a sample script that you can use to create a general certificate template and add it to the Certification Authority. This certificate template allows you to create a single certificate that the AMT platform can use for all of its needs: TLS server authentication, 802.1x, EAC and CIRA. The template's name (as it appears in the CA) is **Intel (R) Platform Configuration**. (In the GUI, the template appears as **IntelPlatformConfiguration**).

This feature is available in Windows 2003 Enterprise Edition using an Enterprise CA.

You run the VBscript from a Command line, giving the CA as a parameter. The new certificate template is then added to Active Directory and to the CA chosen by the user.

A message indicates whether the script was successful. In case of failure, the message indicates an error, and information about the error is written to an error file.

A certificate created using the template can be used by a client or for server authentication.

## Entering a Root Certificate Hash Manually in the AMT Platform's Firmware

Normally the certificate hashes are programmed in the AMT platform's firmware by the OEM. However, there is an option of entering the root certificate's hash manually via the MEBx.

To enter the certificate hash via the MEBx:

- 1 Open the Root certificate and tab to Details. Keep the Root certificate thumbprint from the thumbprint field for later use in step 7.
- 2 Power on the AMT platform and press <ctrl-p> during boot.
- 3 When the MEBx menu is displayed, perform a full unprovisioning.
- 4 Select **Setup and Configuration** and choose **TLS PKI**.
- 5 Choose **Manage Certificate Hashes**.
- 6 Press <Insert> and enter a name for the hash.
- 7 Enter the Root certificate thumbprint from step 1.
- 8 Exit the MEBx and reboot the platform.

## Selecting the Certificate Used by the SCS for Remote Configuration

The SCS only works with one Remote Configuration certificate at a time, matching one of the hashes in the Intel AMT devices in the enterprise. The SCS user performs the following steps to select the desired certificate.

You can insert more than one certificate into the certificate store; the SCS will choose the certificate suitable for the specific AMT platform.

- 1 Install the certificate created above in the Certificate Store of the SCS application user on the platform where the SCS executes. Follow the following steps:
  - a Open certificates (on the local computer) using the Microsoft Management Console (MMC). If you are not logged in as the application user, open MMC using Runas. To add the certificates plug-in to the MMC,
    - Select **file/add snap-in**.
    - Select **Add....**
    - Select **Certificates**.
    - Click **Add**.
    - Select **My user account**; click **Finish**.
    - Select **Close**; select **Certificates** and click **OK**.
  - b In the console tree, open the certificates branch; open the Personal folder and right-click on Certificates.
    - Point to **All Tasks** and then click **Import** to start the Certificate Import Wizard.
    - Type the path and file name of the certificate to be imported or click **Browse** and navigate to the file.
    - Select **Place all certificates in the following store**. The Personal certificate store should already be selected. Click **Next** and **Finish**.



---

**Note:** If the SSL certificate comes from a CA whose "chain of trust" certificates are not automatically included in the Window 2003 trusted certificates store, it will be necessary to install the root certificate and any intermediate certificates in the local computer store on the processor where the SCS executes. To save the root certificate, follow the brief procedure below.

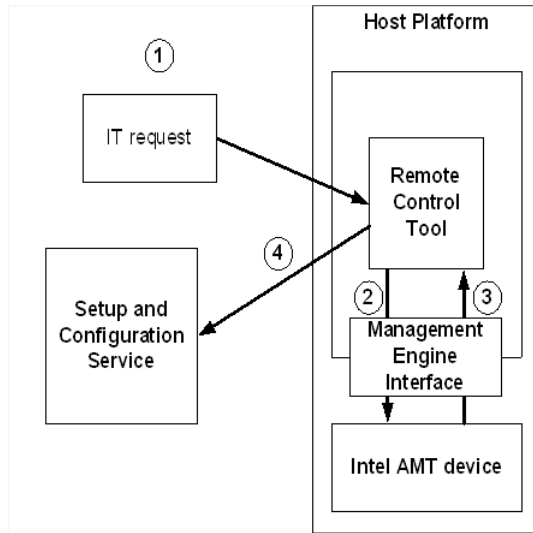
---

### Installing a Root Certificate and Intermediate Certificates on the Server Running the SCS

- 1 Retrieve the root certificate and the certificates of any intermediate CAs, according to the instructions of the certificate vendor. It may be possible to download them from the vendor website, or the vendor may e-mail the trusted root. Save the certificate in .cer format.
- 2 Navigate to each stored certificate and right-click on it. Select **Install certificate**. A certificate manager Import Wizard will appear. Click **Next**.
- 3 Select **Automatically select the certificate store based on the type of the certificate** and click **OK**.
- 4 Click **Next** then **Finish**.
- 5 When prompted and asked if you wish to add the following certificate to the root store, click **Yes**.

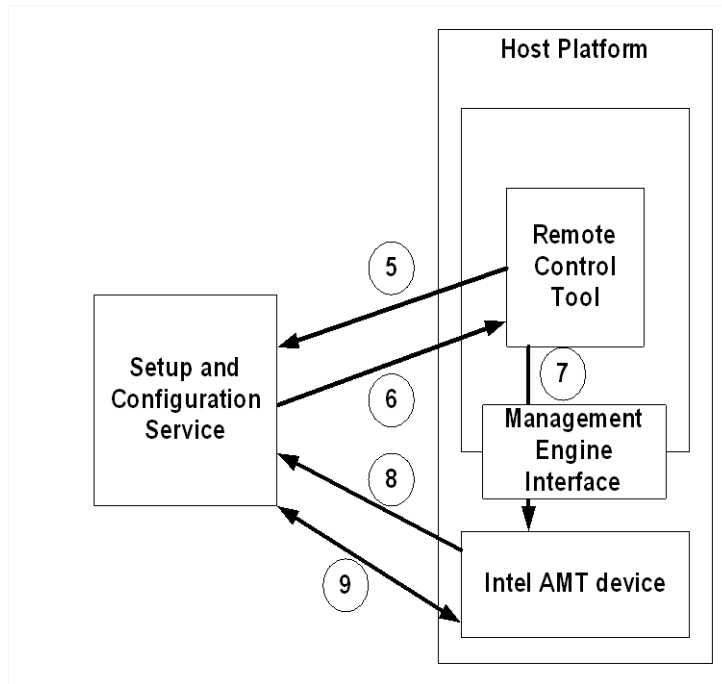
## Steps leading to the Start of Setup and Configuration

Once the above preparations are complete, the following steps are performed:



- 1 IT activates the Intel® vPro™ Technology Activator Utility, via a startup script or an enablement script.
- 2 The Intel® vPro™ Technology Activator Utility detects Intel AMT and requests the UUID and the FQDN.
- 3 Intel AMT device returns the values to the Intel® vPro™ Technology Activator Utility.

- 4 The Intel® vPro™ Technology Activator Utility sends the platform information to the SCS.



- 5 The Intel® vPro™ Technology Activator Utility requests a one-time password (OTP) from the SCS.
- 6 The SCS sends an OTP to the Intel® vPro™ Technology Activator Utility.
- 7 The Intel® vPro™ Technology Activator Utility sends the OTP to the Intel AMT device and commands it to open the network interface. The Intel AMT device generates a self-signed certificate. This process may take up to seven minutes to generate the necessary keys.
- 8 The Intel AMT device starts sending version 3 “Hello” messages.
- 9 Setup and configuration begins using the PKI-CH protocol. The SCS requests the Intel AMT device to send an OTP. The device responds with the value it received from the Intel® vPro™ Technology Activator Utility.

## Remote Configuration Setup and Configuration Process

- 1** After the Intel® vPro™ Technology Activator Utility commands the Intel AMT device to start configuration, the device opens its network interface for 24 hours, and starts sending “Hello” messages. Note: The interface is open for 24 hours (configurable by the OEM) only the first time that it is enabled. If the time runs out before setup and configuration completes or the Intel AMT device is unconfigured or partially unconfigured, any subsequent calls from the Intel® vPro™ Technology Activator Utility to start configuration will open the interface for only six hours.
- 2** The SCS extracts the hashes from the “Hello” message.
- 3** The SCS sends a certificate chain that includes a trusted root certificate matching one of the received hashes.
- 4** The Intel AMT device validates the SCS certificate: It checks that the OID or the OU is correct as described above, and that it is derived from a Certification Authority that matches one of the root certificate hashes.
- 5** The Intel AMT device verifies that the domain suffix matches the DNS suffix in the SCS certificate. (See “Remote Configuration Certificate – Differences between Releases” on page 146.)
- 6** The SCS and the Intel AMT device perform a complete mutual authentication session key exchange:
  - a** The Intel AMT device uses a self-signed certificate, sending its public key.
  - b** The SCS creates a TLS session master key, encrypts it with the Intel AMT device public key, and sends it to the Intel AMT device.
  - c** The device decrypts the master key with its private key. The key is the shared secret used to establish the setup and configuration TLS session.
- 7** One Time Password verification: The SCS requests the OTP from the Intel AMT device. The device sends the OTP securely. The SCS verifies the OTP for correctness.
- 8** Setup and configuration continues. At some point before the SCS sends a CommitChanges command to complete the setup and configuration process, it must send a SetMEBx password command to change the password from its default.
- 9** Since the Intel AMT device network interface is open for a limited period after sending the first “Hello” message, the SCS can command the device to extend this period by up to an additional 24 hours.

## Intel AMT Release 3.0 Additional Features

### Simplified One-Touch

Intel AMT Release 3.0 supports a one-touch configuration mechanism that avoids the possibility of a malicious user masquerading as the SCS. If an IT administrator enters the FQDN of the SCS via the MEBx menu, then in step 5 of “Remote Configuration Setup and Configuration Process”, the Intel AMT device verifies that the FQDN in the SCS client certificate matches the entered value.

### Bare Metal Setup and Configuration

With Intel AMT Release 3.0, a platform containing Intel AMT can be configured by the manufacturer to start sending “Hello” messages as soon as the platform is connected to AC power and to the network. There may be no operating system up and running on the host, thus the name “bare metal”. With no operating system, there is no way to run the Intel® vPro™ Technology Activator Utility to install a One Time Password. This mode allows entering an optional FQDN for the SCS. Either the manufacturer adds it before delivery or an IT administrator adds it, as described in <XREF>Simplified One-Touch. The Intel AMT device will acquire an IP address from a DHCP server, and then start sending “Hello” messages. There is no OTP to exchange in this case; otherwise, the setup and configuration flow is the same. The SCS cannot setup Bare Metal platforms when an OTP is required..

## Remote Configuration Certificate – Differences between Releases

Intel AMT validates the SCS certificate by comparing a domain suffix or FQDN against the CN in the certificate. Different Intel AMT releases perform this comparison differently. This can have an impact on the certificate that an organization acquires. Note that an SCS installation that will set up platforms with a mix of Intel AMT releases will need to acquire a certificate that is appropriate for all the versions that will be configured.

### Intel AMT Release 2.2

Intel AMT retrieves its domain suffix using DHCP Option 15. The CN in the SCS certificate must match the full domain suffix. The result is that a separate certificate is required for each domain.

For example, the CN in the certificate is **corp.east.yourenterprise.com** and DHCP returns a domain suffix of **east.yourenterprise.com**. The CN contains the full suffix so there is a match. A CN of **yourenterprise.com** would not match **east.yourenterprise.com**.

Since an SCS installation can only work with one Remote Configuration certificate at a time, a separate certificate and SCS instance is required for each domain where Intel AMT-based platforms are located.

### Intel AMT Release 3.0

If a Release 3.0 platform depends exclusively on the domain suffix returned by DHCP, it behaves the same as Release 2.2.

The Release 3.0 FQDN option and domain extension option add the following:

- If IT enters the FQDN of the SCS via the MEBx menu or with a formatted USB key or the manufacturer enters the value before delivery, the CN in the certificate must either exactly match all fields of the FQDN or it must be a wildcard entry with a match in all but the first field of the FQDN. For example, if the FQDN is **east.corp.yourenterprise.com**, the CN in the certificate must also be **east.corp.yourenterprise.com** or **\*.corp.yourenterprise.com**.

- If a DSN suffix is entered, then all fields in the suffix must be included in the CN. For example, if the entered suffix is **corp.yourenterprise.com**, then the CN could be **corp.yourenterprise.com** or **east.corp.yourenterprise.com** or **main.east.corp.yourenterprise.com** (but not **east.yourenterprise.com**).

Using one of the above options requires a “single touch,” which should be balanced against the need for an SCS installation and unique certificate for each domain.

## Intel AMT Release 2.6

Release 2.6 supports the 2.2 functionality, with the following additions:

- Wildcard CN: If the CN in the certificate is preceded by “\*.”, then the domain suffix received from DHCP need only match the CN where they have overlapping fields. For example, if the CN is **\*.a.b.org**, then **yyy.a.b.org**, **a.b.org**, and **b.org** would all match (but **c.b.org** would not).
- If the CN ends with “.com” or “.net”, then the domain suffix received from DHCP needs to match only last two fields in the CN. For example, if the CN is **east.corp.yourenterprise.com**, then **west.mkting.yourenterprise.com** would match.
- Release 2.6 supports certificates that use the SubjectAltName (SAN) “DNS Name” extension. The certificates have multiple DNS names, and each one is compared consecutively with the domain suffix received from DHCP. When one of the names matches, Intel AMT accepts the certificate. A certificate with multiple DNS names would be useful when the root domain is not .com or .net.

When one of these methods is used, a single SCS can support Intel AMT devices with Release 2.6 in multiple domains with a single remote configuration certificate.

## Intel® vPro™ Technology Activator Utility

The Remote Configuration process includes the Intel® vPro™ Technology Activator Utility that runs on the host. The Activator Utility is included in the SCS distribution.

For details on using the Intel® vPro™ Technology Activator Utility, refer to the *Intel® vPro™ Technology Activator Utility User's Guide*.





# B

---

## CRL XML Format

The Intel AMT SCS Console can import a Certificate Revocation List (CRL) into a Profile. The following file is an example of the XML format.

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<!--
```

**This file maps the untrusted certificates serial number to the URI of the issuer.**

**The URI value represents a valid CRL distribution point of a Certificate Authority.**

```
-->
```

```
<crl>
```

```
  <uri name="http://crl.myenterprise.com/pki/mscorp/crl/mswww(2).crl">
```

```
    <cert serialnumber="15 27 82 20 00 00 00 00 01"/>
```

```
    <cert serialnumber="15-27-82-20-00-00-00-00-02"/>
```

```
    <cert serialnumber="15278220000000000003"/>
```

```
  </uri>
```

```
  <uri name="http://corppki/crl/mswww(2).crl">
```

```
    <cert serialnumber="15 27 82 20 00 00 00 00 04"/>
```

```
    <cert serialnumber="15 27 82 20 00 00 00 00 05"/>
```

```
  </uri>
```

```
</crl>
```

The serial number attribute must contain the following format:

- Use exactly two hexadecimal characters for each byte (a byte with a single character will be ignored).
- The serial number can be represented as a single hexadecimal number. If the bytes are separated from each other, use any non-hexadecimal character separator between each pair.

The file format is defined with the following XSL style sheet:

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified">

  <xs:element name="cert">
    <xs:complexType>
      <xs:attribute name="serialnumber" type="xs:base64Binary"
        use="required"/>
    </xs:complexType>
  </xs:element>

  <xs:element name="crl">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="uri" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="uri">
    <xs:complexType>
      <xs:sequence>
```

```
        <xs:element ref="cert" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="name" type="xs:string" use="required"/>
</xs:complexType>
</xs:element>
</xs:schema>
```



# C

---

## Using a Script to Import Intel AMT Configuration Properties

When the SCS is configured to use a script to obtain information about an Intel AMT device that sent a setup request, the following occurs:

The Intel AMT device sends a "Hello" message.

- When the SCS receives the "Hello" message, it first searches the New Intel AMT table for a matching UUID entry.
- If there is no matching entry, the SCS sets environment variables based on values in the message.
- The SCS activates the script.
- The script locates the necessary parameters and creates a file consisting of an XML fragment.
- When the script completes, the SCS reads the file and adds an entry to the New Intel AMT table using the values returned by the script in the file.
- The SCS performs setup and configuration using the information in the file.

### Environment Variables

The SCS sets the following environment variables to pass values to a script:

- CS\_AMT\_UUID: The UUID from the Hello message
- CS\_AMT\_STATUS: status of the device to be setup- "U" (Unprovisioned), "I" (In provisioning), or "P" (Already provisioned)
- CS\_AMT\_ADDRESS: The value depends on the value of the previous parameter.

- If CS\_AMT\_STATUS = "U" or "I", CS\_AMT\_ADDRESS = the source IP address from the Hello message.
- If CS\_AMT\_STATUS = "P", CS\_AMT\_ADDRESS = the FQDN of the Intel AMT device to be set up.
- CS\_OUT\_FILE\_NAME: A file name generated by the SCS. The script returns the Intel AMT properties in a file with this name in the same directory as the script in the format described in "Output File Format".

## Output File Format

The output file generated by a script must be an XML fragment interpretable by the SCS. The fragment has the tag **amtConfiguration** and contains the following attributes:

- **fqdn**: The FQDN of the platform containing the Intel AMT device
- **addn**: The Active Directory OU to be used for this device or "NA" when the SCS is not integrated with Active Directory.
- **profile** or **profile\_id**: Either the SCS Profile name or the index of the profile to be used when setting up this device (only one of these can be used).

The file will have the structure shown in the following examples:

```
<amtConfiguration fqdn="jonesr.west.yourenterprise.com"
addn="OU=AMTDevs,DC=west,DC=yourenterprise,DC=com"
profile="Standard_user"/>
```

or

```
<amtConfiguration fqdn="jonesr.west.yourenterprise.com"
addn="OU=AMTDevs,DC=west,DC=yourenterprise,DC=com" profile_id="2"/>
```

## Script Functionality

Script functionality is the responsibility of the ISV or the IT organization. The script may retrieve the information from an external source or from the platform containing the Intel AMT device, or some combination of the two methods. For example, the script may request the FQDN from the platform using the IP address, then determine the Active Directory OU and SCS Profile based on the FQDN.

## Sample Scripts

The SCS distribution includes several sample scripts. They each have advantages and disadvantages. The scripts take two approaches to acquiring the necessary device data. The first approach is a Server Script that requests the data remotely from the platform sending the "Hello" message. The second approach is a pair of scripts: a Client Script that runs on the host processor of a platform containing Intel AMT and requests the platform information and writes it to a database, and a Server Script that reads the database entry and returns it to the SCS. In either case, the controlling enterprise has to modify these scripts for local use.

### Server Script

The Server Script approach requires a copy of the script only on the platform running the SCS. It has the disadvantage of requiring the SCS user to have administrator permissions on every client (see box below).

The SCS distribution includes a script called `GetConfigProperties.vbs`. The script sends a WMI query to the host platform that sent the "Hello" message, and therefore requires that the host is operational and running a version of Microsoft Windows that processes WMI queries.

---

**Note:** The SCS user requires appropriate permissions to invoke WMI remotely. To use this script, the SCS user must be an administrator on the local host (a member of the local Administrators group).

---

The sample script has a 30 second timeout in case WMI freezes on the host; however, the script may require 10 to 20 seconds to execute normally, due to WMI timing on the host.

The script:

- 1** Validates the environment variables.
- 2** Using the WMI protocol, requests the Win32\_ComputerSystemProduct object to recover the platform UUID from the host platform.
- 3** Using the WMI protocol, requests the Win32\_ComputerSystem object to recover the platform name and domain from the host platform.
- 4** Creates the FQDN by concatenating the name and domain.
- 5** Validates that the returned UUID is the same as the UUID environment variable.
- 6** Creates an amtConfiguration XML fragment using the FQDN and a hard-coded OU and profile name.
- 7** Writes the fragment to an output file.

The script is run by executing runscript.bat, which invokes cScript.exe, the command-line version of the Windows script host. The script writes output files to the same directory as the one containing the script and runscript.bat. The distribution also includes testme.bat, a batch file that sets the environment variables and then invokes the script.

On the General Properties pane of the SCS Console, select Get New Intel AMT Properties/Get Intel AMT Configuration from Script and enter the path name to the batch file on each platform running the SCS, for example:

C:\program files\intel\AMTConfserver\scripts\runscript.bat

See “AMT Configuration Parameters” on page 109.



## Client Script

The sample client script has the advantage of requiring only local system privileges. It has the disadvantage of requiring an auxiliary database and deployment to all client platforms. This approach has three elements:

- A database accessible to all machines in the Active Directory group account. Each row in this database contains information about a platform that has Intel AMT on it. The unique key is the UUID. The client platforms only have Add Row privileges to this database. The sample includes an SQL file, `CreateAuxDB.SQL`, that creates the database in SQL Server.
- A client script named `AddConfigPropertiesToAuxDB.vbs` that runs at least once on each client platform. The client script reads the UUID and the FQDN and writes them to the database. In order to run the script on many machines you can use some automatic tools such as Group Policy. The Group Policy will make each AMT platform on the group run the script as soon as the AMT platform starts Windows.
- A server script named `GetConfigPropertiesFromAuxDB.vbs` that searches the database for an entry that matches the UUID in a "Hello" message and returns the UUID, FQDN, Profile name, and Active Directory OU to the SCS. The sample script returns a profile and OU based on the FQDN. The SCS would call this script on receipt of a "Hello" message when there is no entry in the SCS database for the UUID in the "Hello" message.

The client script:

- 1 Sets up script parameters.
- 2 Using the WMI protocol, requests the `Win32_ComputerSystemProduct` object to recover the platform UUID and FQDN.
- 3 Writes a record to the database.

The server script:

- 1 Queries the database using the UUID.
- 2 Erases the row in the database so future updates by the client script will be successful, for example, after changing the FQDN of the platform.
- 3 Builds an XML fragment with the returned parameters.
- 4 Returns the XML fragment to the SCS.

Add the path to the batch file that executes the script to the General Properties page of the SCS Console. As with the server script, `GetConfigPropertiesFromAuxDB.vbs` can be executed with `runscript.bat` and tested with `testme.bat`.

---