Intel® Setup and Configuration Service

Installation and User Guide

Version 6.0

Document Release Date: May 9, 2010

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL 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.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document 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.

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 order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/#/en_US_01

Intel® Active Management Technology requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see here.

Table of Contents

1

Introduction

This guide describes how to install and use the Intel® Setup and Configuration Service (Intel® SCS).

This chapter provides a brief description of the Intel SCS and how you can use it as part of the Intel® Active Management Technology (Intel® AMT) environment.

It includes the following topics:

- About the Intel AMT Environment
- Intel Setup and Configuration Service Components
- Intel AMT and Security Considerations
- Automatic Maintenance

About the Intel AMT Environment

Intel AMT enables you to remotely access computers even when the operating system is unavailable or the computer is turned off. The only requirement is that the computer is connected to a power supply and a network. The Intel AMT environment includes the following:

- **Intel AMT Systems** — Computers based on the Intel® vPro™ chipset that includes a Manageability Engine (ME) and an extended BIOS (MEBx). The ME acts as the interface between the computer and management consoles/the Intel SCS.
- **Intel® vPrO™ Technology Activator Utility** — You run this application on the Intel AMT systems to quickly initiate and send configuration and un-configuration requests to the Intel SCS.

  For more information, see the *Intel® vPro™ Technology Activator Utility Release Notes and User Guide*.
- **Intel SCS** — See “Intel Setup and Configuration Service Components” on page 2.
- **Management Console** — An application that enables you to remotely perform Intel AMT tasks on Intel AMT systems.

Intel Setup and Configuration Service Components

The Intel SCS enables you to automatically configure Intel AMT systems (Intel AMT version 2.0 and later) and includes the following components:

- **Service** — The Windows service *(SCSServer.exe)* that processes the configuration/un-configuration requests sent from the Activator utility or the Console. The configuration is determined by a configuration profile stored in the database.
- **Database** — The secure repository that stores the setup and configuration data, organized according to the Intel SCS database schema, and installed as a database instance in Microsoft SQL Server.
- **Windows Management Instrumentation (WMI)** — The Application Programming Interface (API) used by applications to interact with the Service.
- **Console** — An application that uses the WMI API to communicate with the Service. The Console described in this guide enables you to perform the following:
    - Create and edit configuration profiles used to configure Intel AMT systems.
    - Create and export TLS-PSK configuration keys to enable secure communication between the Intel AMT systems and the Service during configuration.
    - Import TLS-PSK configuration keys supplied by an Original Equipment Manufacturer (OEM).
    - View the status of Intel AMT systems (also known as platforms).
    - Remove Intel AMT configuration settings from Intel AMT systems.
    - Reconfigure Intel AMT systems with different profiles.
    - View the status of the Services and define global and individual Service settings.

  You can install and run the Console from any computer in the network that has access to the computer running the Service.

Intel AMT and Security Considerations

This section describes several topics related to security.

Transport Layer Security Protocol

The Transport Layer Security (TLS) is a protocol that secures and authenticates communications across a public network. Intel AMT uses the following types of TLS:

- **Pre Shared Key (PSK)** — The PSK protocol provides secure communication based on a set of PSK configuration keys that have been shared in advance between two parties using a secure channel. Intel AMT uses the PSK protocol only before and during the configuration process of Intel AMT systems.
- **Public Key Infrastructure (PKI)** — The 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.

How and when these protocols are used depends on the stage in the configuration process and the version of the Intel AMT system, as described in the following:

- "Security Before and During Configuration" on page 3
- "Security After Configuration" on page 4

Security Before and During Configuration

Configuration requests sent from an Intel AMT system to the Intel SCS by the Activator contain sensitive security related information about the network environment. Therefore, Intel AMT uses one of the TLS protocols (PSK or PKI) to ensure authentication and security before and during the configuration process.

The type of TLS protocol you can use during configuration depends on the Intel AMT version:

- **Versions 2.0/2.1/2.5** — You can only use PSK.

  You must change the MEBx password of these Intel AMT systems from the default password. Since entering the PSK configuration key and changing the MEBx password requires a reboot of the Intel AMT system, you can not usually configure these systems remotely.

- **Versions 2.2/2.6/3.x/4.x/5.x/6.0** — You can use PSK or PKI.

  To use PKI, the Intel AMT system must have a Root Certificate Hash pre-programmed in the firmware (usually by the OEM) and you must install a client certificate on the computer running the Service. If you select to use PKI, you can configure the Intel AMT systems remotely using the Remote Configuration feature.

Security After Configuration

Once an Intel AMT system has been configured, the level of security of communication between the Intel AMT system and the Management Console (and the Intel SCS), depends on the settings you defined in the profile used to configure the Intel AMT system.

You can use TLS-PKI in your network to ensure secure communication with all versions of Intel AMT systems. You must provide access to the Microsoft Certification Authority (CA) as the Intel SCS requires it to enroll for certificates on behalf of each Intel AMT system. 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 Intel SCS instance and the Stand-alone CA must be installed on the same server as the Intel SCS.

The TLS-PKI can have a hierarchy of CAs, with subordinate CAs and a root CA. This is beyond the scope of this guide.

Protecting Against Systems Masquerading as Intel AMT Systems

If the Intel SCS receives a request from the Activator for an Intel AMT system that is recorded in the database as having completed setup, the request will be ignored. This protects against a rogue system masquerading as an Intel AMT system waiting for setup. If the Intel AMT system was reset to the Factory Setup (pre-configuration) state by an application other than the Intel SCS or by entering an Un-provision command using the MEBx, then the system must be removed from the database before configuration can take place.

Integration with Active Directory

If your network is using Active Directory, you can define the Intel SCS to configure the Intel AMT systems to use security features of the Active Directory. During configuration, the Intel SCS creates an Active Directory object representing the Intel AMT system and adds it to the Active Directory Organization Unit (ADOU) you defined that contains all Intel AMT systems.

Support for Wireless Environments

The Intel SCS configures Intel AMT systems that support mobile platforms (Intel AMT Releases 2.5, 2.6, 4.0, and 6.0) so that they can receive management traffic over wireless links. The Intel SCS supports defining wireless profiles.

The Intel 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
- Microsoft IAS: With 802.1x EAP-TLS

Automatic Maintenance

For each Intel AMT system successfully setup and configured the Intel SCS performs the following routine maintenance tasks automatically:

- **Clock Synchronization** — Synchronizes the clock in each Intel AMT system to the clock on the computer running the Intel SCS. This task is performed every 10 days.
- **Random Password Change** — If the administrative password and the KVM passwords were created randomly, new random passwords are created. This task is performed every 10 days.
- **ADOU Password Change** — If the Intel SCS is defined to work in Active Directory Integrated mode, the passwords of the ADOU objects representing the Intel AMT systems are changed every 90 days. This task is started at least 10 days before the password is due to expire.
- **Certificate Re-Issue** — If the Intel AMT system contains PKI certificates that are close to the expiry date the certificates are re-issued. This task is started at least 30 days before the certificate is due to expire.
- **Reconfiguration of Intel AMT Systems** — When you change the settings in a configuration profile a new version of the profile is created. The Intel SCS applies the settings of the new profile version to all Intel AMT systems configured with the profile.

These maintenance tasks run at pre-defined intervals or when a change occurs that requires one of the tasks to be performed. Each time the Intel SCS accesses an Intel AMT system it checks and performs any of the tasks that are required. You can also manually run the maintenance tasks on a collection or a single Intel AMT system.

2

Installing the Intel SCS

This chapter describes how to install the Intel SCS.

It includes the following topics:

- About Installing the Intel SCS
- Supported Operating Systems and SQL Versions
- Installation Tasks and Prerequisites
- Installing the Intel SCS Components
- Modifying/Uninstalling the Intel SCS
- Upgrading the Intel SCS
- Actions Required after Upgrade
- Silent Installation
- User Permissions Required to Access the Intel SCS

About Installing the Intel SCS

One installation file (*IntelSCSInstaller.exe*) is used to install all Intel SCS components. Although you can install the Intel SCS components on one computer, for optimized performance Intel recommends that you distribute them across several computers in your network.

Note:

- This version of the Intel SCS does not support the Windows Workgroup environment. If you need to install the Intel SCS in a Windows Workgroup, install the Intel SCS 6.0 Lite version instead.
- If you installed a technology preview of the Intel SCS, you must uninstall it before performing the installation.
- If you are upgrading from an Intel SCS version prior to version 6.0 (or Intel SCS Lite), see “Upgrading the Intel SCS” on page 20 before you continue.

Supported Operating Systems and SQL Versions

The following table describes on which operating systems and SQL versions the Intel SCS components can run.

Table 1. Operating Systems and SQL Versions

Component	Version
Service and Console	• Windows Server* 2003 (all x32/x64 versions) • Windows Server 2008 (all x32/x64 versions) • Windows Server 2008 R2
Console Only	• Windows* XP Professional SP2 (all x32/x64 versions) • Windows Vista* (all x32/x64 versions) • Windows 7 Professional (all x32/x64 versions)
Database	• SQL Server* 2000 Enterprise • SQL Server 2000 (Standard x32 and Enterprise x64) • SQL Server 2005 (Express and Enterprise x32) • SQL Server 2005 (Standard x32/x64 and Enterprise x64) • SQL Server 2008 (Express and Enterprise x32/x64)
* Other names and brands may be claimed as the property of others.	

Note: To run the Intel SCS InstallShield wizard, .NET Framework version 2.0 must be installed on the computer.

Installation Tasks and Prerequisites

The tasks that you must perform and the prerequisites you require to install the Intel SCS depend on which features of the Intel SCS you want to implement and how your network infrastructure is configured.

The following table describes the tasks and prerequisites.

Table 2. Installation Tasks and Prerequisites

To do this...	You need to...
Install the Intel SCS	• Have local administrator privileges on the computers where you want to install Intel SCS components. • To run the Intel SCS InstallShield wizard, .NET Framework version 2.0 must be installed on the computer. • Ensure that the Microsoft SQL Server where you will store the database is one of the supported versions listed in Table 1. • Create a user account to run the Service. For a list of the permissions that the Service account user requires to run the Service, see "Service User Account Requirements" on page 10. • Install the Intel SCS components (see "Installing the Intel SCS Components" on page 11). • Ensure that all users that will need to access the Intel SCS have the required permissions (see "User Permissions Required to Access the Intel SCS" on page 30).
Use the Console	Ensure that .NET Framework version 2.0 is installed on the computer where you want to run the Console.
Use the Activator Wizard	• Ensure that .NET Framework version 2.0 is installed on the computer where you want to run the Activator Wizard. • Copy the *Activator* folder to the computer.
Integrate the Intel SCS with Active Directory	• Create an Organizational Unit (OU) in Active Directory to store objects containing information about the Intel AMT systems. In a multiple domain environment, Intel recommends that you create an OU for each domain. • Give *Create*/*Delete* permissions in the OU you created to the user account running the Intel SCS. • Define how the Intel SCS will integrate with the Active Directory (see "Defining Service Settings" on page 36).

Table 2. Installation Tasks and Prerequisites (Continued)

To do this...	You need to...
Use the Transport Layer Security (TLS) protocol when communicating with Intel AMT systems	To implement these features you must install and configure Microsoft's Certificate Authority (CA) on a computer in the network. For more information see "Certification Authorities and Templates" on page 113.
Use the IEEE802.1x network protocol to authenticate Intel AMT systems and define Endpoint Access Control (EAC) settings	
Use the remote access feature	
Setup and configure Intel AMT systems using the remote configuration feature	See "Remote Configuration" on page 104.

Additional Requirements for Windows 2003 CA

If the Service is installed on a server running Windows Server 2008 (all x32/64 versions and R2) and the CA is installed on a server running Windows Server 2003, perform the following:

1. On the computer running the CA, select **Start** > **Run** > **Dcomcnfg**.
2. Select **Component Services** > **Computers**.
3. Right-click My Computer and select **Properties**.
4. Select the **COM Security** tab.
5. In the Access Permissions section, click **Edit Limits**.
6. Select the Service user account and grant it the following permissions:
    - Local Access
    - Remote Access

Installing the Console on a Network Drive

Due to security measures built into .NET Framework, when you try to start a Console installed on a network drive, you might receive the following error message:
Intel (R) AMTSCS Console has encountered a problem and needs to close.

To solve this problem, you must enable "Full Trust" for the network share as shown in the following example:

```
cd c:\WINDOWS\Microsoft.NET\Framework\v2.0.50727
CasPol.exe -m -ag 1.2 -url file:///N:/your/network/path/* FullTrust
```

Connecting to a Service behind a Firewall

If you install the Service on a computer that is protected by a firewall, you might receive error messages when you try to connect to the Service. You must ensure that the firewall is configured to enable the WMI to connect to the Service.

For more information, refer to the Microsoft Developer Network:

http://msdn.microsoft.com/en-us/library/aa389286(VS.85).aspx

Service User Account Requirements

The user account running the Service requires the following on the server where the Service (*SCSServer.exe*) is installed:

- *Full Control* permission on the following registry key:

  HKEY_LOCAL_MACHINE > SOFTWARE

  (From the Registry Editor, right-click the key and select **Permissions**).
- *Log on as a service* permission.

  (Select **Start** > **Administrative Tools** > **Local Security Policy** > **Local Policies** > **User Rights Assignment**).
- Write permission on the folder where the Service is installed (the default folder is *C:\Program Files\Intel\AMTConfService*).

The InstallShield wizard attempts to grant these permissions to the Service user you select during installation (Figure 2).

Note: If the Service is installed on server running Windows Server 2008 (all x32/64 versions and R2) the user account must be a Local Administrator on the computer running the Service.

If you want to use scripts to process Hello messages (see "Send a Configuration Request to the Intel SCS" on page 41), the user account running the Service must also:

- Have sufficient permissions on the remote server where the script is located to run scripts.
- Exist as a user in the Console with the *Edit* privilege on System configuration data (see "Creating Intel SCS Users" on page 43).

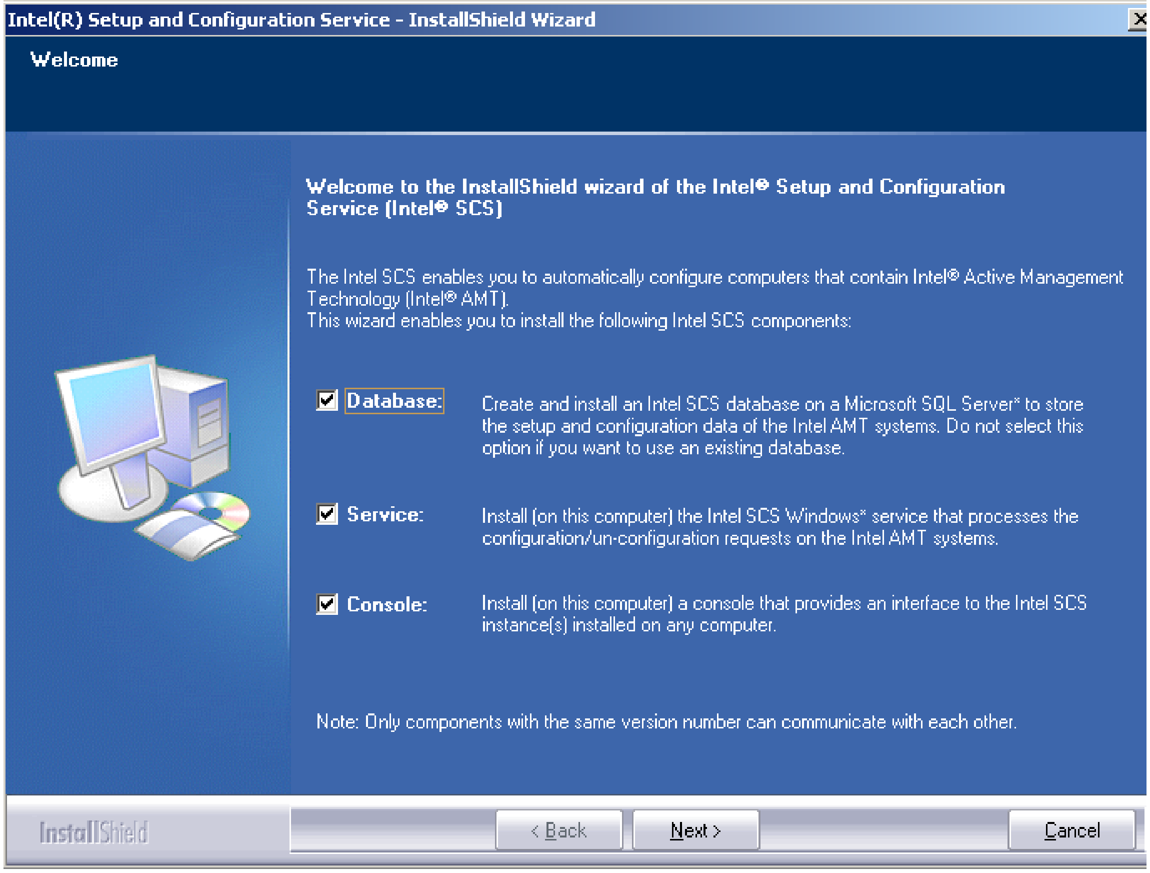
Installing the Intel SCS Components

The following procedure describes how to install all of the Intel SCS components. For each computer/installation you can select the components you want to install.

Note: In order to install the Service or launch the Console, you must either have a pre-installed database or also install the database.

To install the Intel SCS components:

1. Double-click **IntelSCSInstaller.exe**. The Welcome window of the InstallShield wizard appears.



Intel(R) Setup and Configuration Service - InstallShield Wizard

Welcome

Welcome to the InstallShield wizard of the Intel® Setup and Configuration Service (Intel® SCS)

The Intel SCS enables you to automatically configure computers that contain Intel® Active Management Technology (Intel® AMT).
This wizard enables you to install the following Intel SCS components:

☑ Database: Create and install an Intel SCS database on a Microsoft SQL Server* to store the setup and configuration data of the Intel AMT systems. Do not select this option if you want to use an existing database.

☑ Service: Install (on this computer) the Intel SCS Windows* service that processes the configuration/un-configuration requests on the Intel AMT systems.

☑ Console: Install (on this computer) a console that provides an interface to the Intel SCS instance(s) installed on any computer.

Note: Only components with the same version number can communicate with each other.

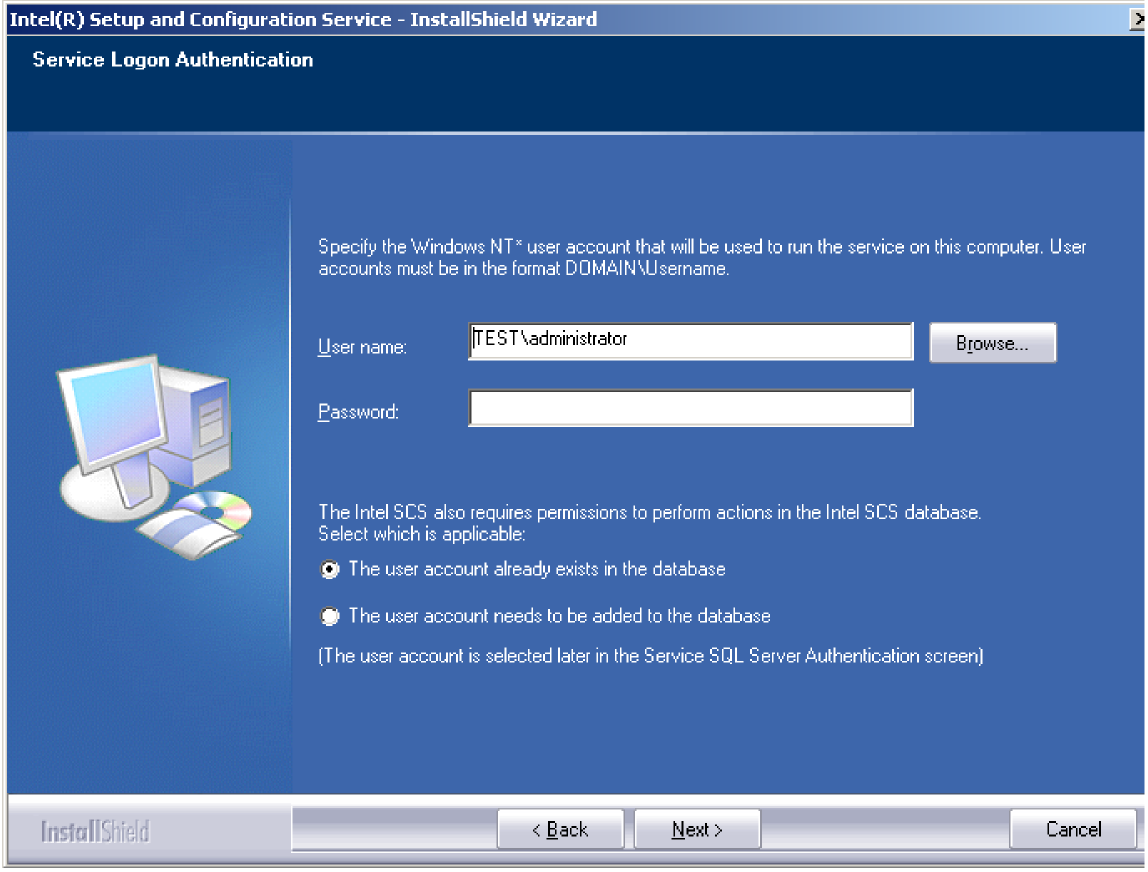
Figure 1. Welcome Window

2. Ensure that only the check boxes of the components that you want to install are selected. You can install any of the following:
   - **Database** — Installs the database on the SQL server that you select. Select this option only once since all the instances of the Intel SCS share the same database.(Do not select this option if you want to use an existing database.)
   - **Service** — Installs the Service.
   - **Console** — Installs the Console. You can install this component on any computer that can connect to the computer running the Service.

3. Click **Next**. The License Agreement window appears.

4. Select **I accept the terms of the license agreement** and click **Next**.

5. If you selected to install the Service, the Service Logon Authentication window appears. This window enables you to define the user under which the Service will run on this computer.



Intel(R) Setup and Configuration Service - InstallShield Wizard

Service Logon Authentication

Specify the Windows NT* user account that will be used to run the service on this computer. User accounts must be in the format DOMAIN\Username.

User name: TEST\administrator

Password:

The Intel SCS also requires permissions to perform actions in the Intel SCS database. Select which is applicable:

● The user account already exists in the database

○ The user account needs to be added to the database

(The user account is selected later in the Service SQL Server Authentication screen)

Figure 2. Service Logon Authentication window

a. Click **Browse** to select the user, or enter the user name (in the format *domain\username*), and then enter the password.

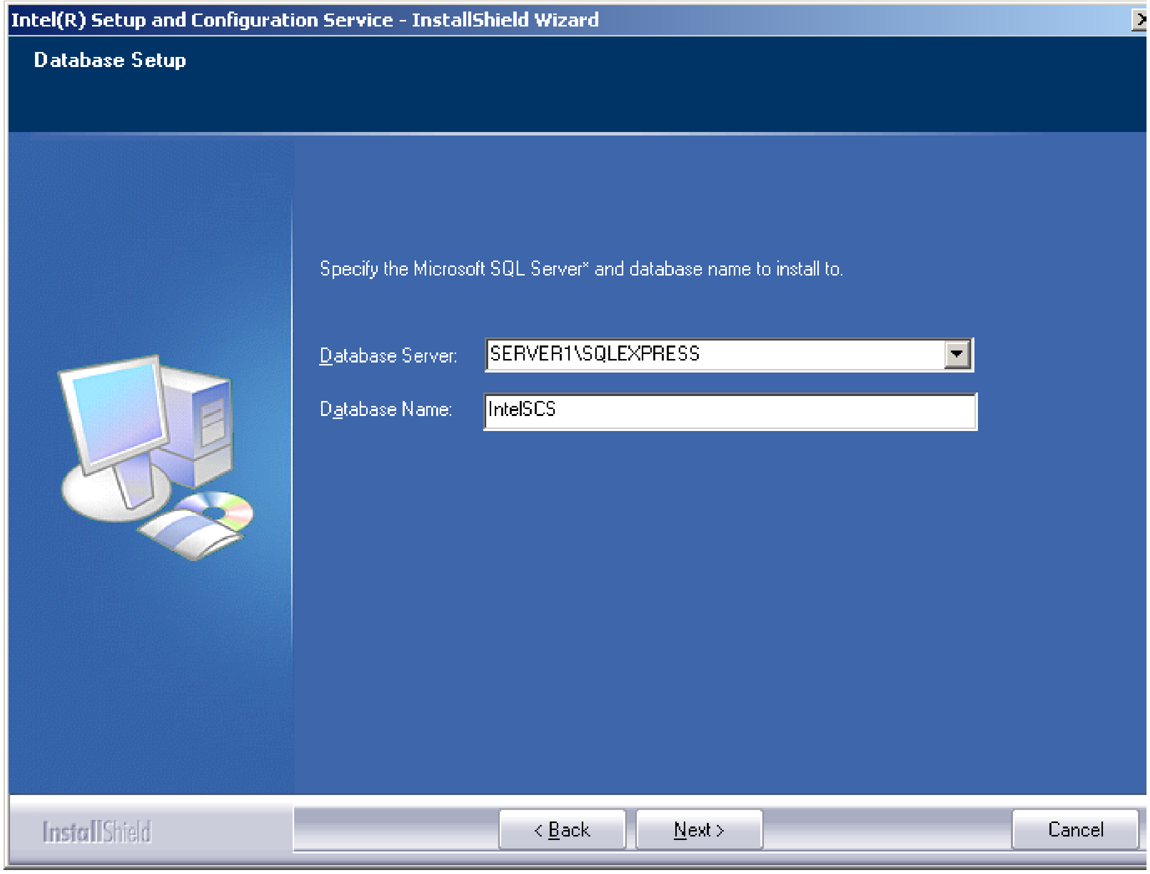
b. If in step 2 you selected the Service check box but did not select the Database check box (because the database already exists), additional fields are displayed regarding the user that the Service will use to connect to the database. Select one of the following:

- **The user account already exists in the database**
- **The user account needs to be added to the database**

c. Click **Next**.

Note: For a list of the permissions that the Service account user requires to run the Service, see "Service User Account Requirements" on page 10.

6. If you selected to install the database or the Service, the Database Setup window appears. This window defines where the database is located (or will be installed if you selected to install).



Intel(R) Setup and Configuration Service - InstallShield Wizard
Database Setup
InstallShield
< Back
Next >
Cancel

Specify the Microsoft SQL Server* and database name to install to.

Database Server: SERVER1\SQLEXPRESS

Database Name: IntelSCS

Figure 3. Database Setup Window

a. In the Database Server field, enter the name of the SQL server that will host the database. If you are performing the installation on the actual SQL server, you can select the server from the drop-down list.

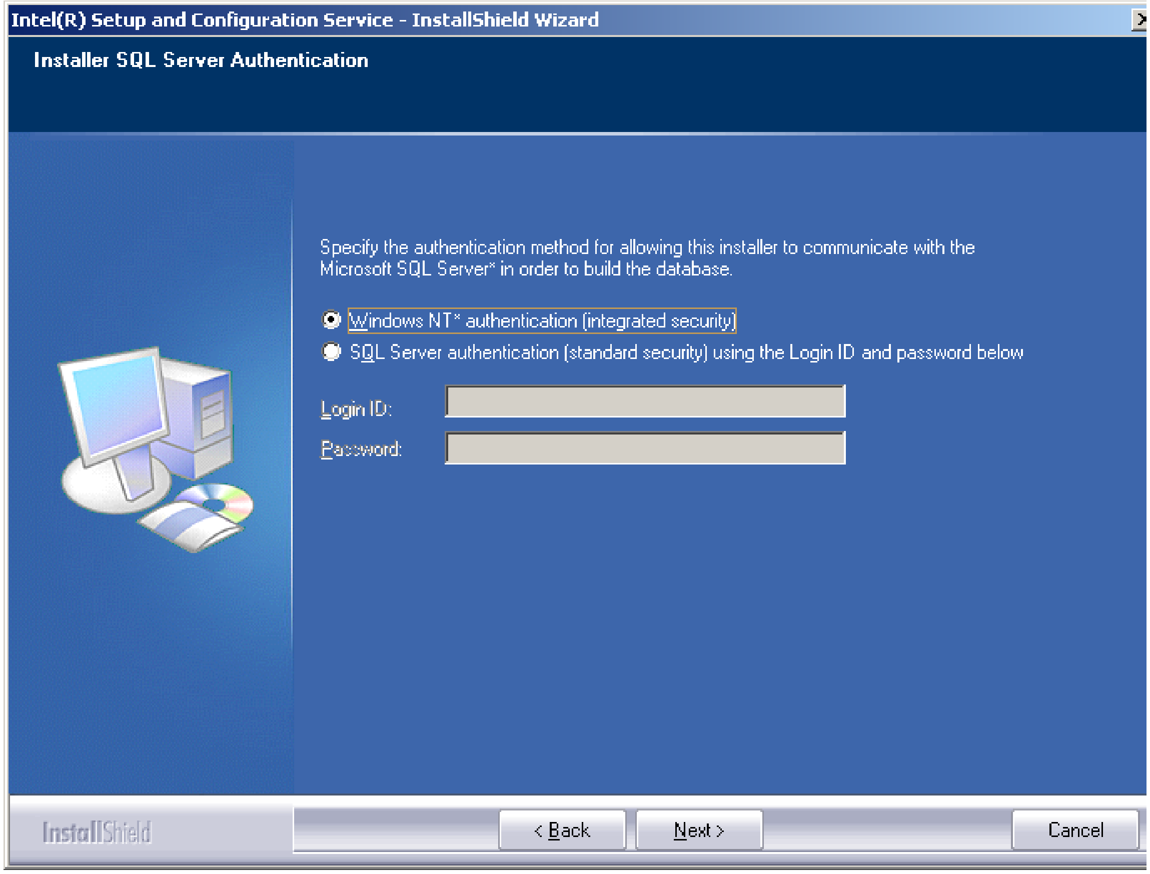
b. In the Database Name field, enter the name of the database to which the Service must connect. If you selected to install the database, the installation creates the database with this name.

c. Click **Next**.

7. Perform one of the following:

- If you did not select to install the database, continue to step 9.
- If you selected to install the database, or the Service user account needs to be added to the database (see step 5b), continue to step 8.

8. If you selected to install the database or the Service user account needs to be added to the database (see step 5b), the Installer SQL Server Authentication window appears. This window defines how the installer will authenticate with the SQL server in order to create or modify the database (or add a Service user).



Intel(R) Setup and Configuration Service - InstallShield Wizard

Installer SQL Server Authentication

Specify the authentication method for allowing this installer to communicate with the Microsoft SQL Server* in order to build the database.

● Windows NT* authentication (integrated security)

○ SQL Server authentication (standard security) using the Login ID and password below

Login ID:

Password:

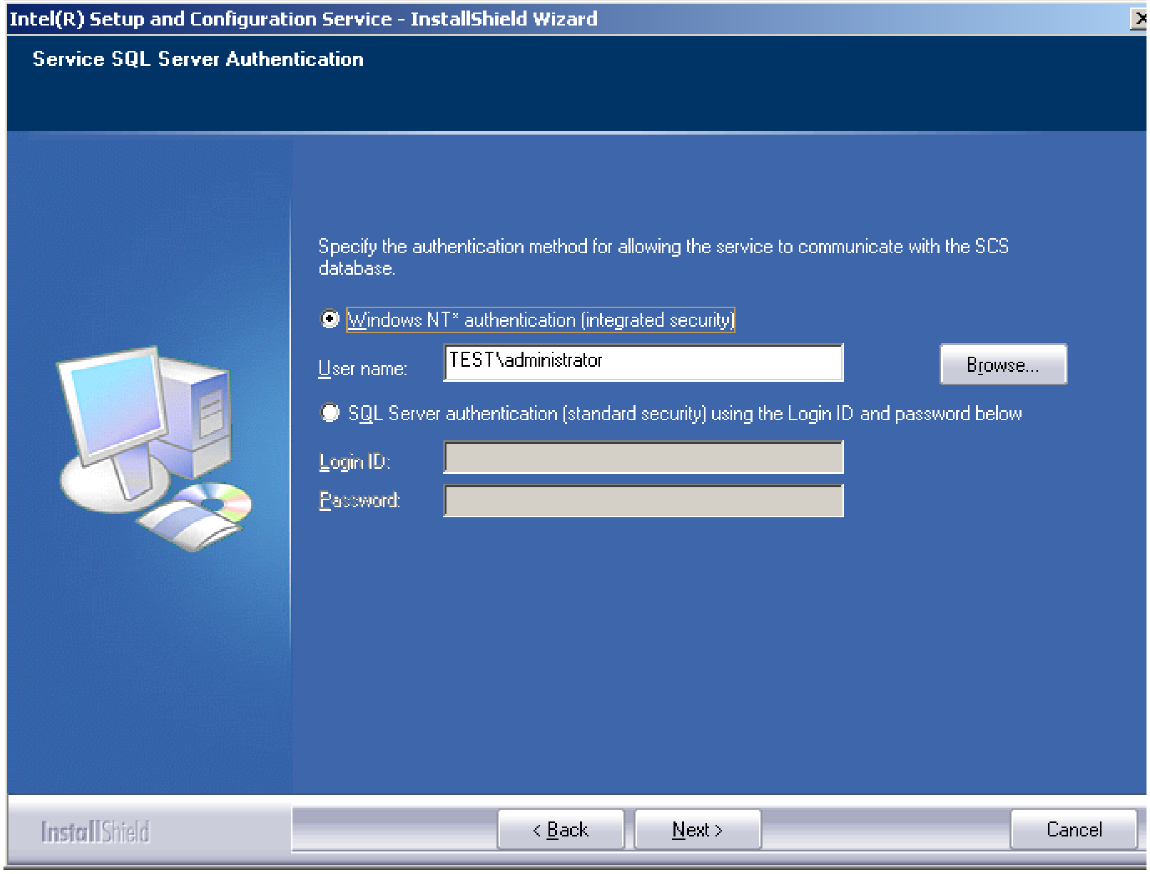
Figure 4. Installer SQL Server Authentication Window

a. Select one of the following authentication methods:

- **Windows NT* authentication** — Authenticate with the credentials of the user performing the installation. If you select this option, you must have sufficient permissions on the SQL server to create or modify a database and add users.
- **SQL Server authentication using Login ID and password below** — If you select this option, enter a user name and password. Ensure that the password meets the password policy requirements of the SQL server.

b. Click **Next**.

9. The Service SQL Server Authentication window appears. This window defines how the Service will authenticate with the database.



Intel(R) Setup and Configuration Service - InstallShield Wizard

Service SQL Server Authentication

Specify the authentication method for allowing the service to communicate with the SCS database.

● Windows NT* authentication (integrated security)

User name: TEST\administrator

○ SQL Server authentication (standard security) using the Login ID and password below

Login ID:

Password:

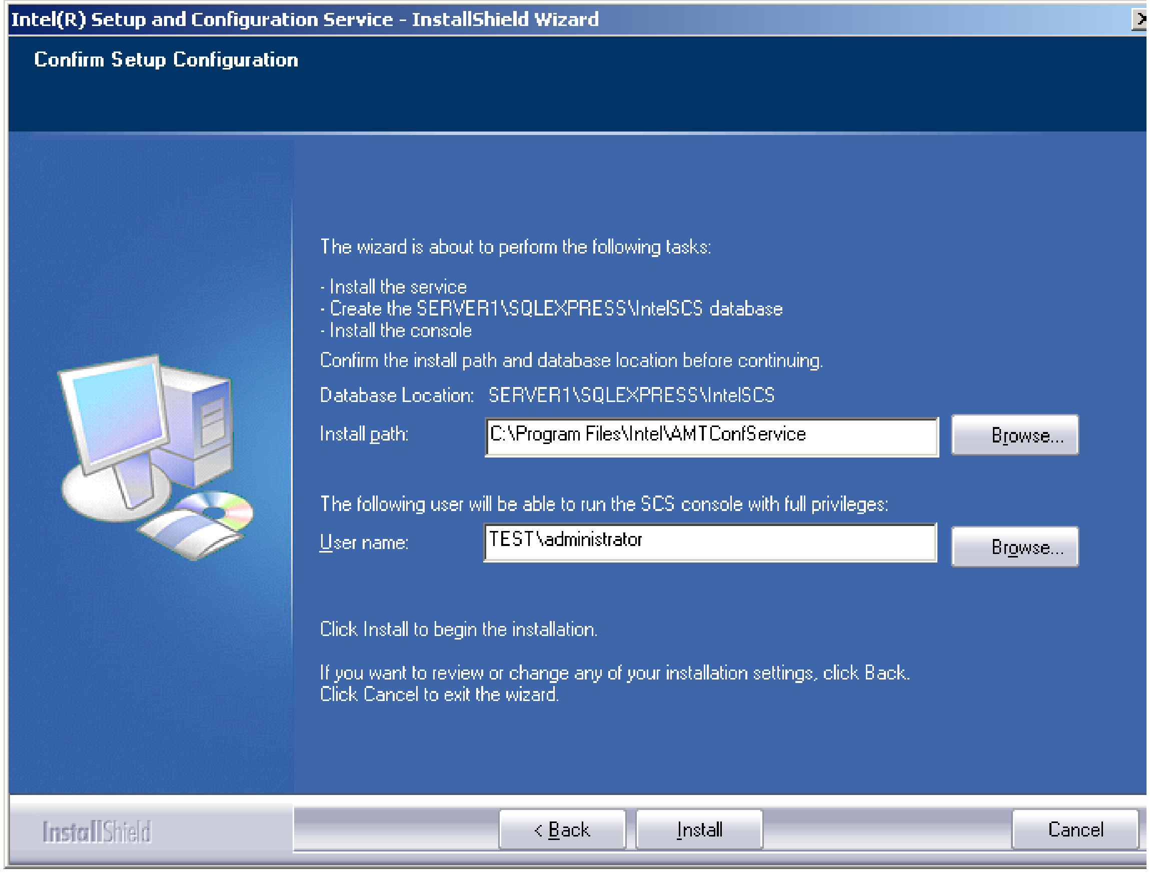
Figure 5. Service SQL Server Authentication Window

a. Select one of the following authentication methods:

- **Windows NT* authentication** — If you selected to install a Service, the user you defined in the Service Logon Authentication window (Figure 2) will be used to authenticate with the SQL server. If you selected to install a database without installing a Service, an additional field is displayed (User name) where you can define the user.
- **SQL Server authentication using Login ID and password below** — If you select this option, enter a user name and password. Ensure that the password meets the password policy requirements of the SQL server.

b. Click **Next**.

10. The Confirm Setup Configuration window appears. This window displays information about the selections you made and enables you to change certain default installation settings.



Intel(R) Setup and Configuration Service - InstallShield Wizard

Confirm Setup Configuration

The wizard is about to perform the following tasks:

- Install the service
- Create the SERVER1\SQLEXPRESS\IntelSCS database
- Install the console

Confirm the install path and database location before continuing.

Database Location: SERVER1\SQLEXPRESS\IntelSCS

Install path: C:\Program Files\Intel\AMTConfService

The following user will be able to run the SCS console with full privileges:

User name: TEST\administrator

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back.
Click Cancel to exit the wizard.

Figure 6. Confirm Setup Configuration Window

a. Optionally, in the Install path field enter the path to the folder where you want to install the Intel SCS components or click **Browse** to select it. The default installation folder is *C:\Program Files\Intel\AMTConfService*.

b. In the User name field, enter the name of the user that will have full privileges in the Console. This user will be added to the database and can be used to create and edit other users (see “Defining Users in the Intel SCS” on page 42).

Note:

- Ensure that this user is a Domain User (and not a Local User).
- Until you create additional users, the user you select here is the only user that can launch the Console.

c. Click **Install**. The installation starts. When the installation finishes, the InstallShield Wizard Complete window appears.

11. Click **Finish**. The InstallShield Wizard closes.

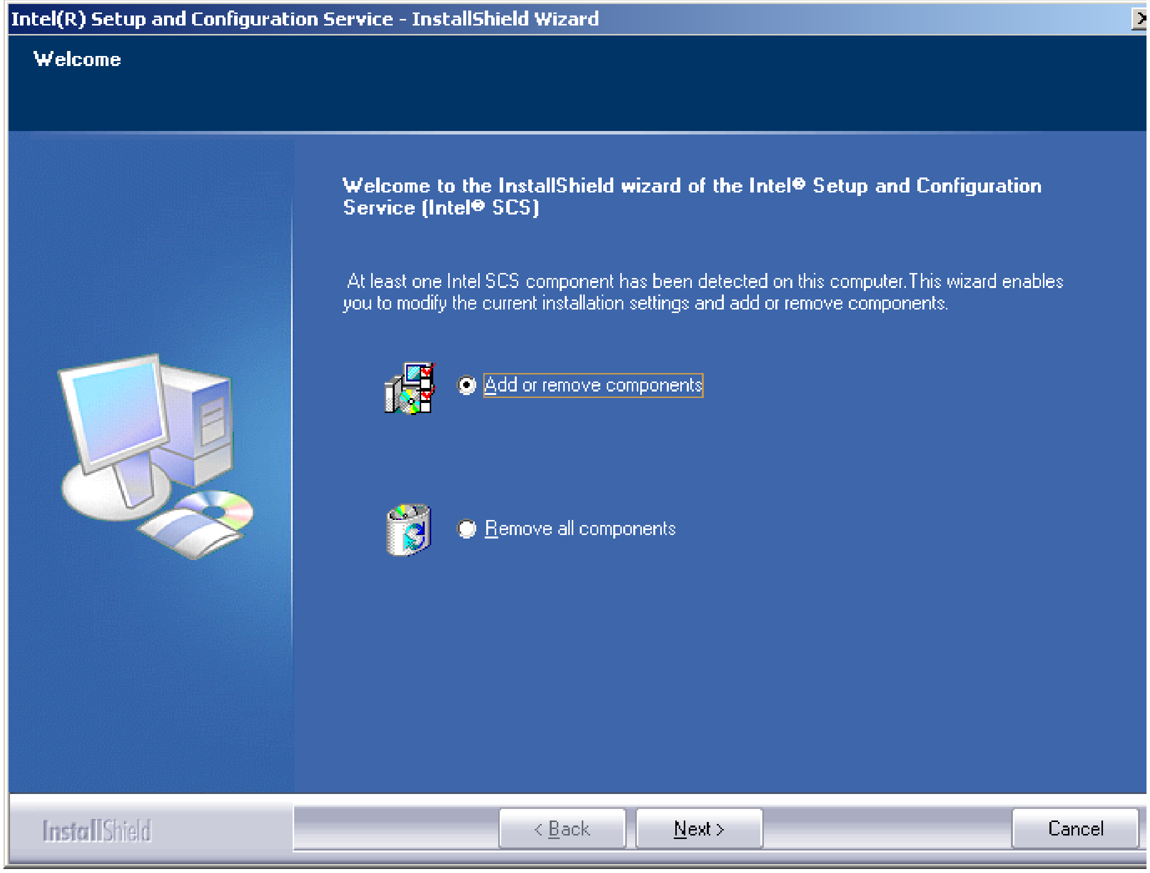
Modifying/Uninstalling the Intel SCS

You can run the installation procedure to change various properties of the installation or remove all the Intel SCS components.

To modify/uninstall the Intel SCS:

1. Double-click **IntelSCSInstaller.exe**. The Welcome window of the InstallShield wizard appears.

Note: You can also perform modify/uninstall from the Add or Remove Programs option of the Control Panel.


Intel(R) Setup and Configuration Service - InstallShield Wizard
Welcome

Welcome to the InstallShield wizard of the Intel® Setup and Configuration Service (Intel® SCS)

At least one Intel SCS component has been detected on this computer. This wizard enables you to modify the current installation settings and add or remove components.

● Add or remove components

○ Remove all components

InstallShield
< Back
Next >
Cancel

Figure 7. Welcome Window

2. Select one of the following:
   - **Add or remove components** — Enables you to modify an existing installation. Continue to step 4.
   - **Remove all components** — Removes all Intel SCS components installed on this computer and the database that you select. Continue to step 3.

3. Click **Next**. A message appears asking if you are sure that you want to remove all the Intel SCS components. Perform the following:

   a. Click **Yes**. The message closes and the Database Setup window appears (Figure 3).

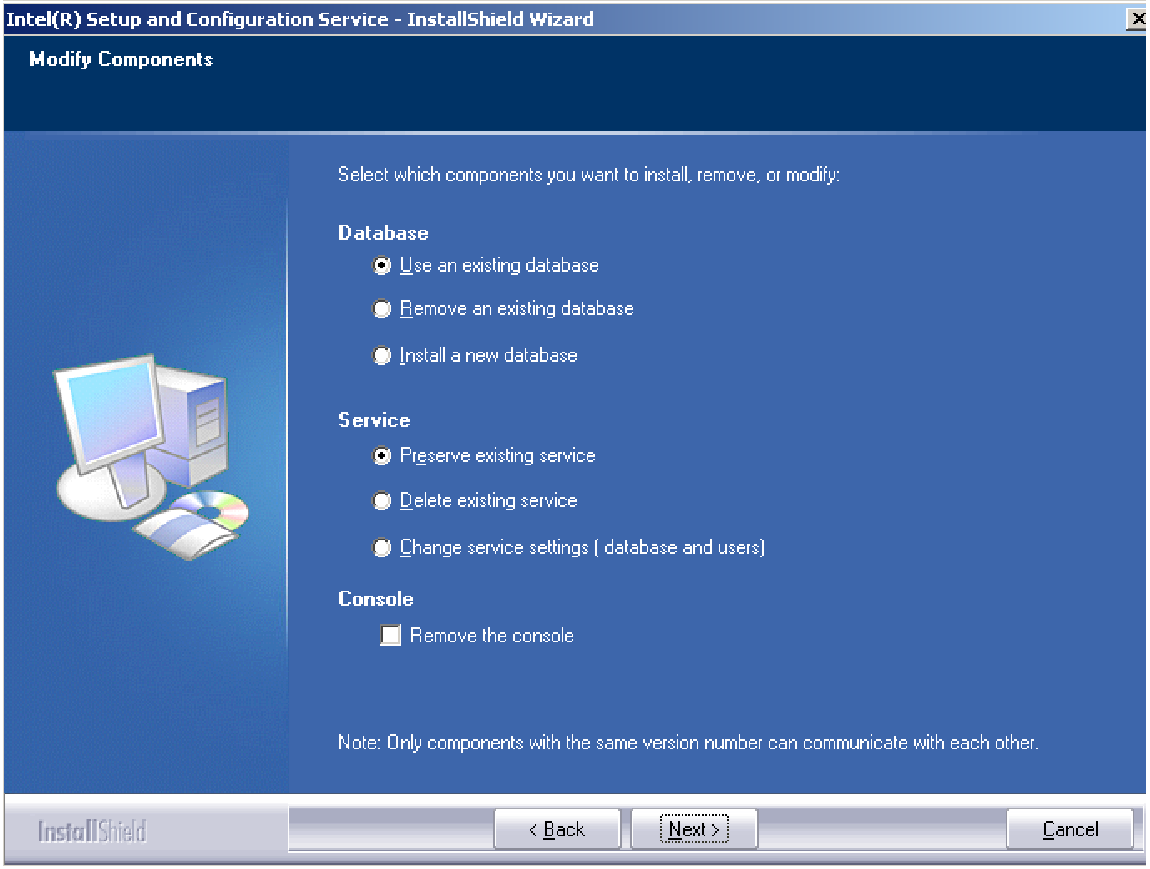
   b. Select the database you want to remove and click **Next**. The Installer SQL Server Authentication window appears (Figure 4).

   c. Define how the installer will authenticate with the SQL server in order to remove the database and click **Next**. A message appears asking if you are sure that you want to delete the database.

   d. Click **Yes**. All the Intel SCS components are removed and the InstallShield Wizard Complete window appears.

   e. Continue to step 8.

4. Click **Next**. The Modify Components window appears. The options that appear in this window depend on which components the InstallShield Wizard detects are installed on this computer.



Intel(R) Setup and Configuration Service - InstallShield Wizard

Modify Components

Select which components you want to install, remove, or modify:

Database

● Use an existing database

○ Remove an existing database

○ Install a new database

Service

● Preserve existing service

○ Delete existing service

○ Change service settings (database and users)

Console

□ Remove the console

Note: Only components with the same version number can communicate with each other.

Figure 8. Modify Components Window

5. For each of the components, select the required option as described in the following table.

Table 3. Modify Components Options

Component	Option
Database	Select one of the following: • **Use an existing database** — Use the existing database. • **Remove an existing database** — Enables you to select and delete a database. Note that if you delete a database that a Service/Console is connected to, the Service/Console will no longer function. • **Install a new database** — Enables you to install an additional database (for example for test purposes). Note that no data is transferred from the existing database. If the Service component is also installed on this computer, the user running the Service will be configured to use this new database.
Service	Select one of the following: • **Preserve existing service** — Use the existing Service installed on this computer. • **Delete existing service** — Deletes the Service from this computer. • **Change service settings (database and users)** — Enables you to make changes to the database, user, and the authentication method that this Service uses.
Console	Depending on if the Console is installed on this computer or not, one of the following check boxes will appear: • **Remove the console** — Select only if you want to remove the Console from this computer. • **Install the console** — Select only if you want to install the Console on this computer.

6. Click **Next** to continue the installation. Enter the required details as described in “Installing the Intel SCS Components” on page 11.

   When complete, the Confirm Setup Configuration window appears.

7. Click **Modify**. The installation starts. When the installation finishes, the InstallShield Wizard Complete window appears.

8. Click **Finish**. The InstallShield Wizard closes.

Upgrading the Intel SCS

Read the following sections carefully before starting to upgrade to Intel SCS version 6.0:

- Moving from Intel SCS Lite to Intel SCS
- About Upgrading from Intel SCS Version 3.x and Earlier
- About Upgrading from Intel SCS Version 5.x
- Prerequisites for Upgrading the Database to Version 6.0
- Performing the Upgrade
- Profile Validation and Incompatible Data

Moving from Intel SCS Lite to Intel SCS

Intel SCS Version 6.0 is distributed as two separate installation packages:

- Intel SCS (this package)
- Intel SCS Lite

Intel SCS does not support direct upgrade from Intel SCS Lite. If you installed the Intel SCS Lite version, and used it to configure Intel AMT systems, you can perform the following steps to transition to Intel SCS:

1. Use the Activator Utility to send unconfiguration requests from each of the configured Intel AMT systems to the Intel SCS Lite.
2. Record the settings that you defined in the Intel SCS Lite configuration profiles.
3. Install the Intel SCS Service component on a Server running one of the supported operating systems.
4. Install the Intel SCS database component on an Server running one of the supported SQL versions.
5. Install the Intel SCS Console component on a computer that can connect to the Service, and create new configuration profiles in the Intel SCS.
6. Use the Activator Utility to send configuration requests from each of the Intel AMT systems to the Intel SCS.
7. When all the Intel AMT systems have been successfully configured by the Intel SCS, uninstall the Intel SCS Lite components.

About Upgrading from Intel SCS Version 3.x and Earlier

Intel SCS 6.0 does not support direct upgrade from Intel SCS versions 3.x or earlier. These versions of the Intel SCS must be upgraded to Intel SCS 5.x (latest version) before they can be upgraded to Intel SCS 6.0.

Before upgrading to version 5.x, perform a backup of the database. After upgrading the database to version 5.x, ensure that the data is correct and intact before continuing the upgrade to version 6.0 (described in the following sections).

About Upgrading from Intel SCS Version 5.x

Upgrading the Intel SCS from version 5.x to version 6.0 involves moving the data from the existing database to a new database schema. The database upgrade is performed only once since all the instances of the Service share the same database. If the database is managed by a DBA, the DBA can upgrade the database using the *IntelSCSInstaller.exe* directly on the SQL server or from a remote computer.

Note: Only Intel SCS components with the same version number can communicate with each other. Intel recommends that you first upgrade the database, and then all instances of the Service and Console. (You can also upgrade local Service and Console installations when upgrading the database.)

Prerequisites for Upgrading the Database to Version 6.0

Ensure that you perform the following steps before upgrading the database from version 5.x to version 6.0.

1. Perform a backup of the database.

   Note: Intel SCS events and log history records are not transferred to the upgraded database.

2. VLANs are not supported in version 6.0 of the Intel SCS. If the **Use VLAN** option of previous Intel SCS versions was used to configure Intel AMT systems, you must reconfigure these systems without VLAN. Remove the setting in the configuration profile (located in the Advanced profile settings window) and reconfigure the systems.

   Note:

   - Configuration profiles with the **Use VLAN** option enabled are NOT transferred to the upgraded database.
   - If you remove the VLAN setting in the configuration profile without ensuring that all the systems were reconfigured, systems that remain defined with VLAN will not be transferred to the new database. These systems will also no longer be accessible from the Intel SCS and can only be reconfigured via their MEBx.

3. Do NOT perform operations on collections prior to starting the upgrade. Where possible, ensure that all operations on single systems and collections have completed.
4. Stop all instances of the Service.

Performing the Upgrade

The following procedure describes how to upgrade from Intel SCS version 5.x to version 6.0.

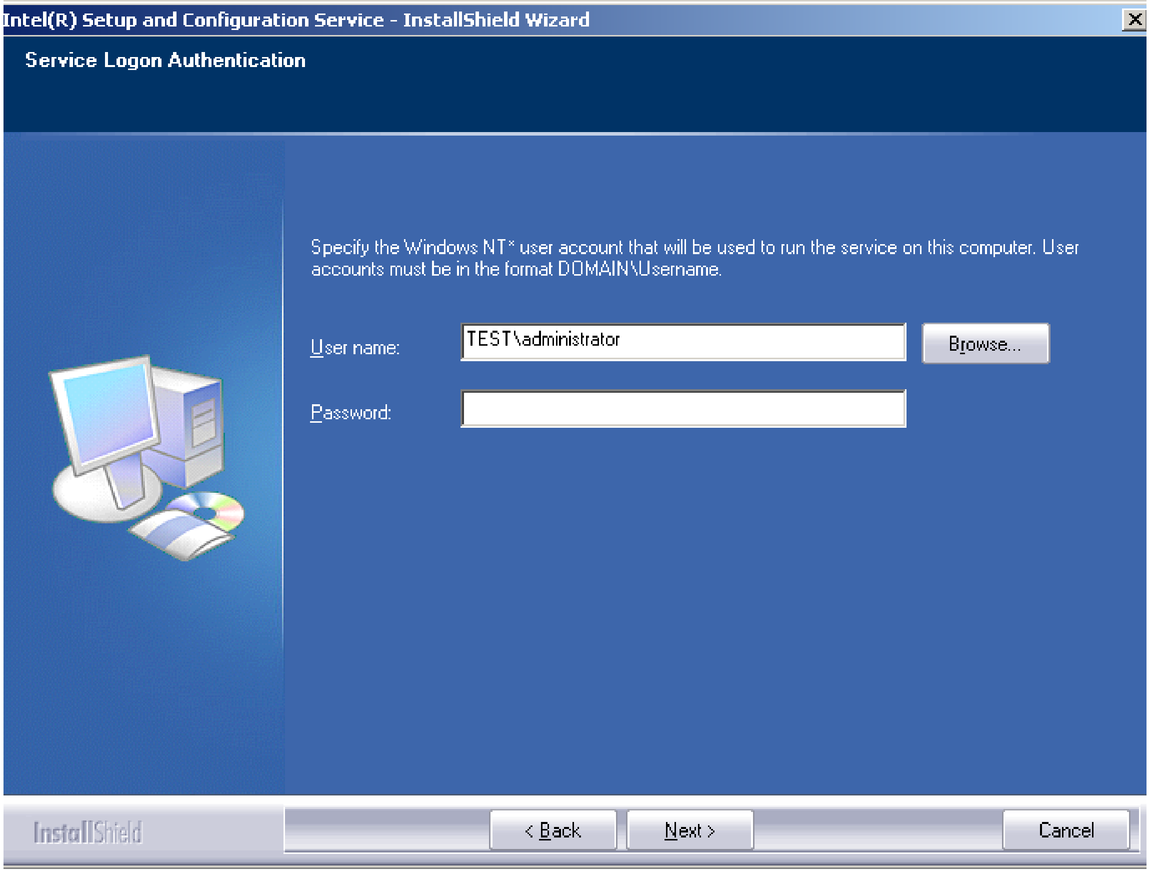
Note: After performing the upgrade, ensure that you check if you need to perform any of the tasks described in "Actions Required after Upgrade" on page 27.

To upgrade the Intel SCS:

1. If you intend to upgrade the database, ensure that a backup of the database was performed.
2. Double-click **IntelSCSInstaller.exe**. The Upgrade Components window of the InstallShield wizard appears with information about the existing Intel SCS version.

   Note: If the installation is started on a computer that has no Intel SCS components installed on it (or they were installed with a script), the InstallShield cannot detect that this is an upgrade and therefore the Welcome window appears (Figure 1). In this case, when performing the database upgrade, ensure that you select the database component in the Welcome window and then select the correct database to upgrade in the Database Setup window (Figure 3).

3. Click **Next**. The License Agreement window appears.
4. Select **I accept the terms of the license agreement** and click **Next**.
5. If a Service is installed on this computer, the Service Logon Authentication window appears. This window enables you to define the user under which the Service will run.


Intel(R) Setup and Configuration Service - InstallShield Wizard
Service Logon Authentication
InstallShield
< Back
Next >
Cancel
Browse...

Specify the Windows NT* user account that will be used to run the service on this computer. User accounts must be in the format DOMAIN\Username.

User name: TEST\administrator

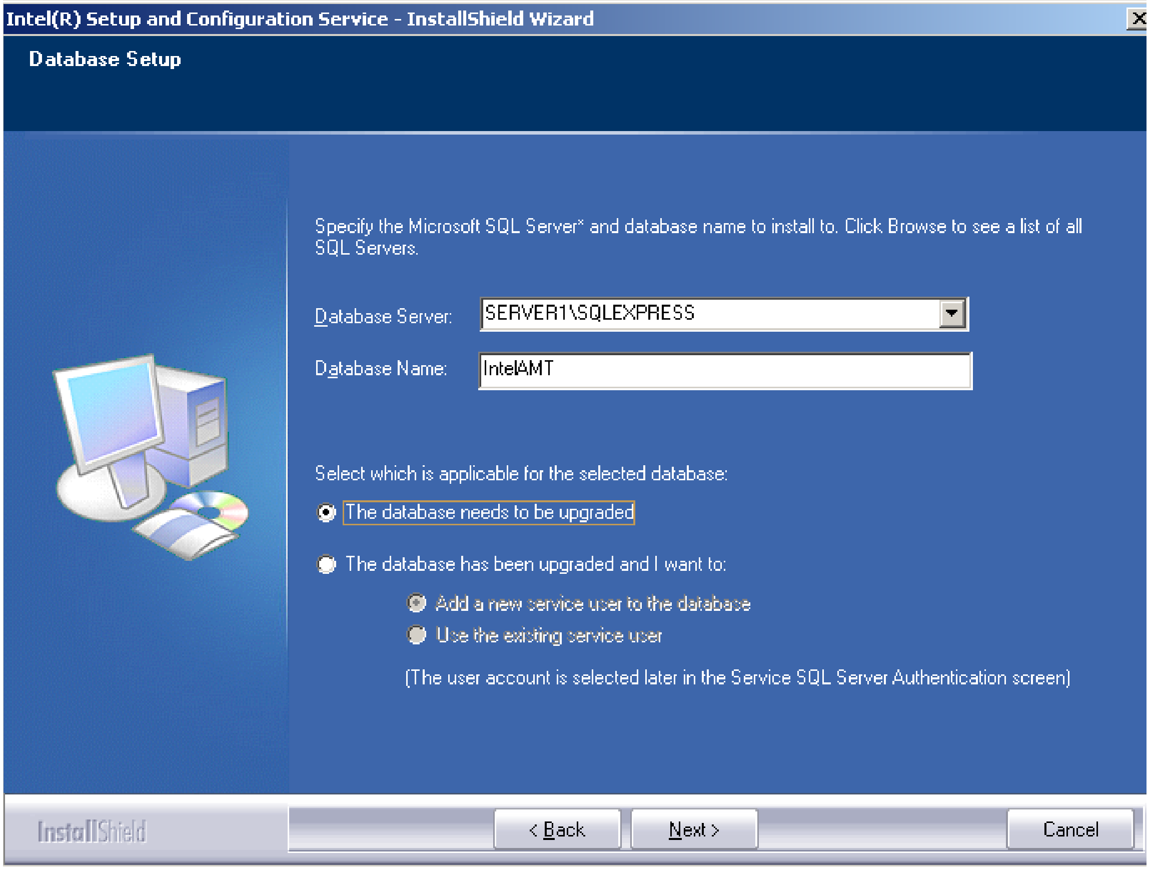
Password:

Figure 9. Service Logon Authentication window

a. Click **Browse** to select the user, or enter the user name (in the format *domain\username*), and then enter the password.

b. Click **Next**.

6. The Database Setup window appears. This window defines where the database is located and what action the upgrade needs to perform.



Intel(R) Setup and Configuration Service - InstallShield Wizard

Database Setup

Specify the Microsoft SQL Server* and database name to install to. Click Browse to see a list of all SQL Servers.

Database Server: SERVER1\SQLEXPRESS

Database Name: IntelAMT

Select which is applicable for the selected database:

● The database needs to be upgraded

○ The database has been upgraded and I want to:

○ Add a new service user to the database

○ Use the existing service user

(The user account is selected later in the Service SQL Server Authentication screen)

Figure 10. Database Setup Window

a. In the Database Server field, enter the name of the SQL server that hosts the database. If you are performing the upgrade on the actual SQL server, you can select the server from the drop-down list.

b. In the Database Name field, enter the name of the database to which the Service must connect.

c. The InstallShield requires information about the database since at this stage it cannot verify the database’s state. Select from the following:

- **The database needs to be upgraded** — Select this option if the database has not yet been upgraded.
- **The database has been upgraded and I want to** — Select this option if the database has already been upgraded, and select if you want the Service to use the existing user credentials to authenticate with the SQL sever or add a new user.

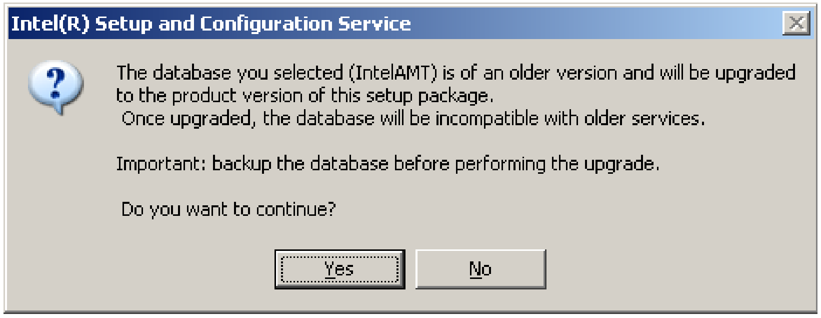
d. Click **Next**.

7. If you selected to upgrade the database or the Service user account needs to be added to the database (see step 5b), the Installer SQL Server Authentication window appears (Figure 4). This window defines how the installer will authenticate with the SQL server in order to upgrade the database (or add a Service user).

   a. Select one of the following authentication methods:

   - **Windows NT* authentication** — Authenticate with the credentials of the user performing the upgrade. If you select this option, you must have sufficient permissions on the SQL server to create a database.
   - **SQL Server authentication using Login ID and password below** — If you select this option, enter a user name and password. Ensure that the password meets the password policy requirements of the SQL server.

   b. Click **Next**. The following message will appear if the database needs to be updated.



The database you selected (IntelAMT) is of an older version and will be upgraded to the product version of this setup package.
Once upgraded, the database will be incompatible with older services.

Important: backup the database before performing the upgrade.

Do you want to continue?

Figure 11. Database Upgrade Window

Ensure that the name of the database is correct and click **Yes** to continue with the upgrade. The InstallShield checks the validity of the configuration profiles in the database. If data exists that is not compatible with the Intel SCS 6.0 database schema the Profiles Validation window appears.

Note: If the Profile Validation window appears, see "Profile Validation and Incompatible Data" on page 26 for instructions before continuing.

8. The Service SQL Server Authentication window appears (Figure 5). This window defines how the Service user will authenticate with the database.

   Select one of the following authentication methods:

   - **Windows NT* authentication** — The user you defined in the Service Logon Authentication window (Figure 9) will be used to authenticate with the SQL server. If you selected to add a new Service user, an additional field is displayed (User name) where you can define the user.
   - **SQL Server authentication using Login ID and password below** — If you select this option, enter a user name and password. Ensure that the password meets the password policy requirements of the SQL Server.

9. Click **Next**. The Confirm Setup Configuration window appears. This window displays information about the selections you made and enables you to change certain default installation settings.
10. From the Confirm Configuration Setup window, click **Upgrade**. When the upgrade finishes, the InstallShield Wizard Complete window appears.
11. Click **Finish**. The InstallShield Wizard closes.
12. Check if you need to perform any of the tasks described in "Actions Required after Upgrade" on page 27.

Profile Validation and Incompatible Data

When upgrading a database from version 5.x to version 6.0 the data is checked for validity with the new database schema before any changes are made to the existing Intel SCS components. If invalid data is found, a log file (*ProfilesValidation.log*) is created with a record for each incompatibility with details of the profile and the severity.

Table 4. Profile Validation Incompatibility

Severity	Description
Information	The data will be upgraded automatically without making any changes to the actual data values.
Warning	The data will be upgraded automatically but a value or setting will be changed.
Error	Required data is missing or not legal, and cannot be upgraded. You must manually change or replace this data.
Critical	The profile contains settings that are no longer supported. If you continue with the upgrade, the profile will be deleted and the Intel SCS will not be able to communicate systems configured with this profile. (The systems will also not exist in the database and it will not be possible to configure them using the Intel SCS.)

The data records are saved into **.CSV* files (with the name of the table in the database). The log file and the *.CSV files are saved in the following folder of the user account performing the upgrade:

\Application Data\Intel_Corporation\SCS_Installer\DB_Conversion

The Profiles Validation window enables you to select from the following:

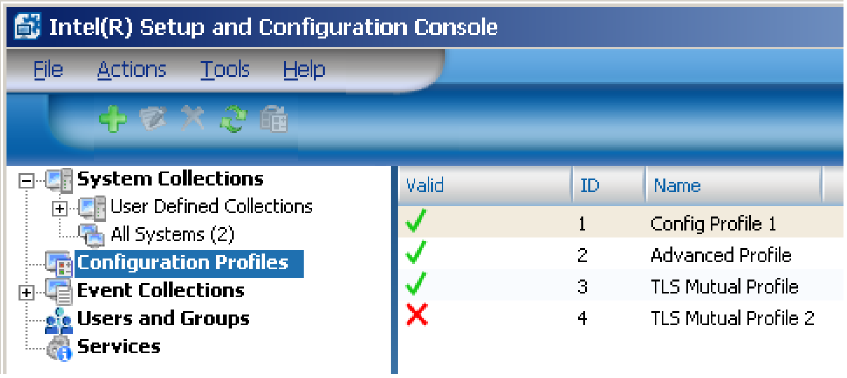
- **View log** — Displays the log file. View the details and decide if you want to continue or abort the upgrade.
- **Abort** — Aborts the upgrade. None of the Intel SCS components that you selected are changed in any way. If you select this option, you can make adjustments in the database (according to the log file) and then restart the upgrade.
- **Continue** — Continue the upgrade installation. If you select this option, the Intel SCS components are upgraded. When upgrade is complete, update the invalid data in the profiles (see "Actions Required after Upgrade" on page 27).

Actions Required after Upgrade

After upgrading the Intel SCS from a version earlier than version 6.0, ensure that you perform the following tasks.

Check for Invalid Configuration Profiles

If the upgrade installation found errors in the configuration profiles (see "Upgrading the Intel SCS" on page 20) and you continued the upgrade, the profiles that contain invalid or missing data are marked in the *Configuration Profiles* node with an ✗. (When all profiles are valid, the Valid column is not displayed.) No operations can be performed on systems configured with invalid profiles, including automatic maintenance.



Valid	ID	Name
✓	1	Config Profile 1
✓	2	Advanced Profile
✓	3	TLS Mutual Profile
✗	4	TLS Mutual Profile 2

Figure 12. Invalid Profile Example

You must edit each invalid profile to correct or add the missing data (see "Defining Configuration Profiles" on page 47). The fields with invalid or missing data are marked with red text in the Configuration Profile Wizard. After you make the required corrections to a profile, the Intel SCS creates a new version of the profile and automatically reconfigures all configured systems with the new profile version.

Check for Systems in a "Failed" Status

For systems that failed configuration in SCS 5.x, or the Intel SCS failed to connect to them, the upgrade process performs the following:

- If the failure occurred within 90 days before the upgrade, the systems are placed in the appropriate "pending" status: *Pending Configuration*, *Pending Configuration Update*, *Pending Unconfiguration*. Automatic maintenance will attempt to perform the required operations on each of these systems within a random period of 2-14 days.
- If the failure occurred more than 90 days before the upgrade, the systems are placed in the appropriate failed status: *Configuration Failed*, *Configuration Update Failed*, *Unconfiguration Failed*. These systems must be dealt with manually.

From the *All Systems* node of the Console tree, search for systems with a "failed" status and decide what action you need to take for each one. You can group these systems into collections and perform operations on them as described in "Viewing and Editing Intel AMT Systems" on page 82.

Check the Users and Privileges

Privileges in the Intel SCS (Console and API) are no longer defined using “Roles”. Instead, you can now define the exact privileges you want to grant to each user/group. The upgrade process grants users with the *Enterprise Administrator* role all privileges. The remaining roles are granted privileges according to Table 5.

- Users with the *Configuration Client* role are granted privileges to edit and remove Intel AMT systems.
- Users with the Administrator role are granted privileges to run Maintenance operations.

Table 5. Version 5.0 Roles Conversion to Version 6.0 Privileges

Privilege/Role	Administrator	Operator	Log Viewer	Configuration Client
System configuration data	Edit and View	Edit and View	-	Edit and View
Configuration profiles	View	View	-	View
Users	-	-	-	-
Service settings	-	-	-	-
PSK data	Edit and View	Edit and View	-	Edit and View
Perform system operations	Enabled	-	-	-
View secure system and profile data	Enabled	-	-	-
View logs	Enabled	Enabled	Enabled	-

Define Hello Message Based Configuration Settings

Note: This task is only relevant in environments using “Hello” messages to setup and configure Intel AMT systems (see “Send a Configuration Request to the Intel SCS” on page 41).

In previous versions, by default the Service always listened for Hello messages from Intel AMT systems. The TCP listener port and the location of a script were defined globally (in Tools > Settings). From version 6.0, if you want to configure using Hello messages, you must define the settings for each Service (the upgrade does not transfer the settings). Also, if you defined a script to process the Hello messages, you must create a new script and enter the path to the new script.

For more information, see “Defining Individual Service Settings” on page 37.

Silent Installation

The InstallShield* executable used to install the Intel SCS, enables you to also install the Intel SCS from a command line using a script file to respond to the installer questions. This capability is called “silent install”. You can also embed the script file into another application (for example, a management console) that will run the silent installation as part of its own installation.

You generate the install script by running the installer with the Record (r) option. Besides installing Intel SCS, this option also causes the creation of an install script that includes the responses that you entered during the installation process.

To perform a silent install:

1. From the command line, run the installation executable file with the following parameters:

   ```
   IntelSCSInstaller.exe /r /f1“<path\silentinstall.iss>”
   ```

   where <path\silentinstall.iss> is the name and location of the install script that you want to create.

   The Welcome window of the InstallShield wizard appears.

2. Perform the required installation, as described in “Installing the Intel SCS Components” on page 11.

3. If the environment on which you want to perform a silent install differs from that of the system on which the install script was recorded, open the script file in a text editor and edit the required parameter values.

4. Once you have an install script suitable for your environment, you can use it to perform a silent install. From the command line, run the installation executable file with the following parameters:

   ```
   IntelSCSInstaller.exe /s /f1“<path\silentinstall.iss>” /f2“<path\scsinstall.log>”
   ```

   where:

   - <path\silentinstall.iss> is the name and location of the install script that you created (and customized if necessary).
   - <path\scsinstall.log> is the name and location of the log file that you want to create. The log file provides information on the installation’s progress and any errors that may occur. For more information, refer to: http://helpnet.acresso.com/robo/projects/installshield11helplib/SetupLog.htm

Note: Use absolute paths and ensure that there are no spaces between the fl or f2 parameters and the first double quotation mark (“).

User Permissions Required to Access the Intel SCS

If a user has administrator permissions on the computer running the Service they will be able to connect to the Service. If you do not want to give a user administrator permissions you can perform the following procedures instead:

- "Defining DCOM Permissions" on page 30
- "Defining WMI Permissions" on page 32

Note: If the Service is installed on an operating system with User Account Control (Windows Server 2008), you must perform both of these procedures even if the user account has administrator permissions.

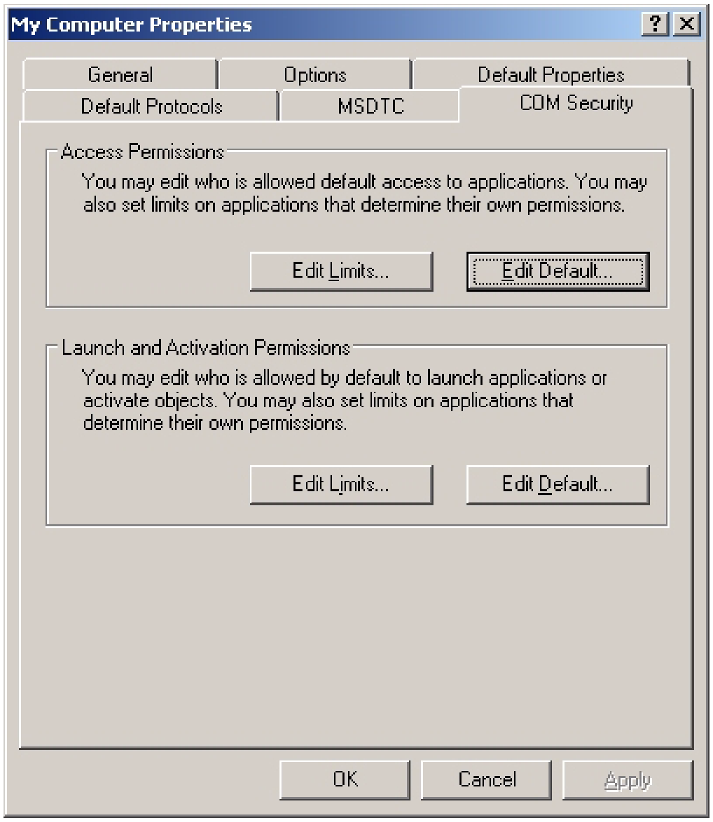
Once a user is connected to the Service, the tasks that he can perform in the Intel SCS (from the Console or the API) are controlled by privileges that you grant to the user (see "Defining Users in the Intel SCS" on page 42).

Defining DCOM Permissions

The following procedure describes how to define DCOM permissions.

To define DCOM permissions:

1. On the computer running the Service open a command prompt window, enter *dcomcnfg* and press <Enter>. The Component Services window appears.
2. From the Console Root tree, select **Component Services** > **Computers** > **My Computer**.
3. Right-click **My Computer** and select **Properties**. The My Computer Properties window appears.
4. Click the **COM Security** tab. The COM Security tab appears.



You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.

Figure 13. COM Security Tab

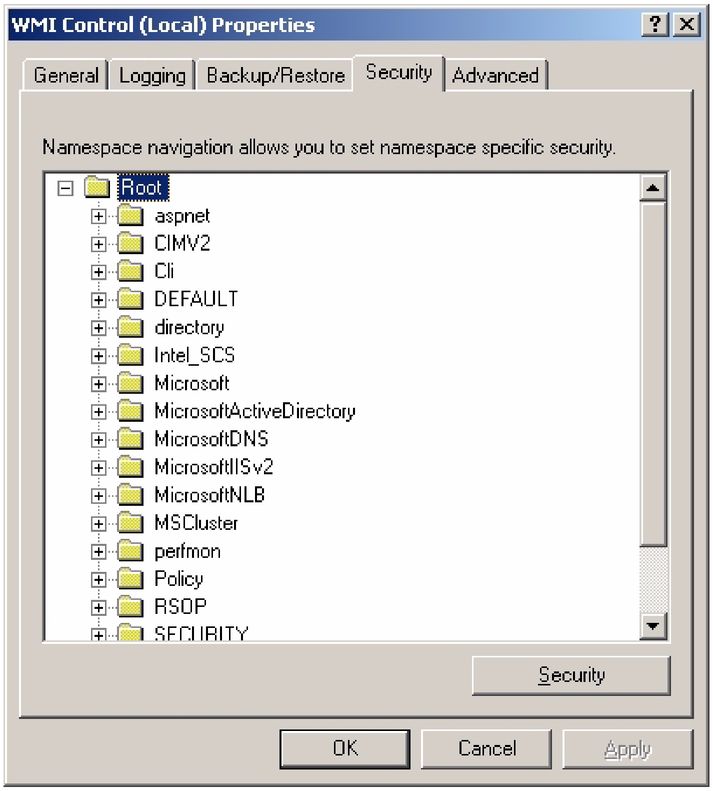
5. From the Access Permissions section, perform the following:
   a. Click **Edit Limits**. The Access Permission window appears.
   b. Ensure that all users that need to connect to the Service appear in the list and have the *Local Access* and *Remote Access* permissions.
   c. Click **OK**. The Access Permission window closes.
6. From the Launch and Activate Permissions section, perform the following:
   a. Click **Edit Limits**. The Launch Permission window appears.
   b. Ensure that all users that need to connect to the Service appear in the list and have the following permissions: *Local Launch*, *Remote Launch*, *Local Activation*, and *Remote Activation*.
   c. Click **OK**. The Launch Permission window closes.
7. Click **OK**. The My Computer Properties window closes.
8. Close the Component Services window.

Defining WMI Permissions

The following procedure describes how to define WMI permissions.

To define WMI permissions:

1. On the computer running the Service open a command prompt window, enter *wmimgmt.msc* and press <Enter>. The Windows Management Infrastructure window appears.
2. Right-click **WMI Control (Local)** and select **Properties**. The WMI Control (Local) Properties window appears.
3. Click the **Security** tab. The Security tab appears.



Namespace navigation allows you to set namespace specific security.

Figure 14. Computer Management Window

4. From the tree, select **Root** and click **Security**. The Security for Root tab appears.
5. Ensure that all users that need to connect to the Service appear in the list and have the *Execute Methods*, *Full Write*, and *Remote Enable* permissions.
6. Click **OK**. Security for Root tab closes.
7. From the tree select **Root** > **Intel_SCS** and click **Security**. The Security for Root\Intel_SCS window appears.
8. Ensure that all users that need to connect to the Service appear in the list and have the *Execute Methods*, *Full Write*, and *Remote Enable* permissions.
9. Click **OK**. The Security for Root\Intel_SCS window closes.
10. Close the Windows Management Infrastructure window.

3

Quick Start Guide

This chapter provides a quick start guide for setting up and using the Intel SCS.

It includes the following topics:

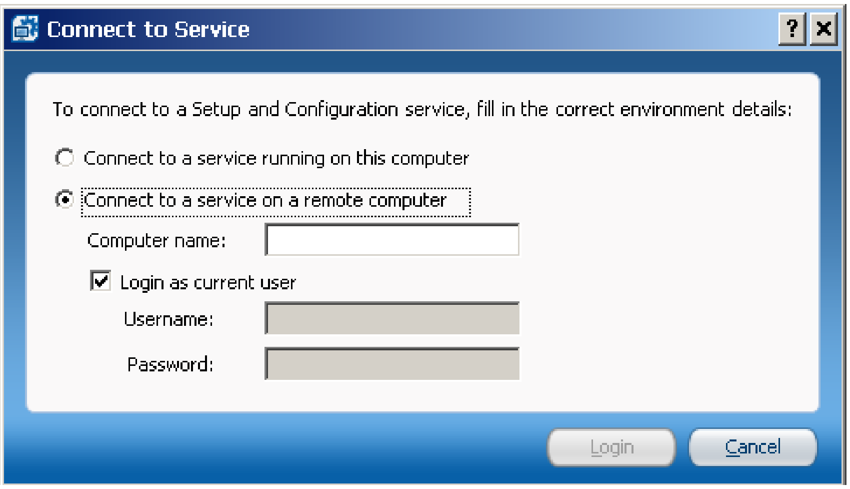
- Starting the Console and Connecting to a Service
- Defining Service Settings
- Defining Console Settings
- Configuring an Intel AMT System

Starting the Console and Connecting to a Service

When you start the Console for the first time, you must provide details on how your environment is defined. The next time you start the Console it will automatically login.

To start the Console:

1. Double-click **SCSConsole.exe**. The Connect to Service window appears.



Connect to Service

To connect to a Setup and Configuration service, fill in the correct environment details:

○ Connect to a service running on this computer

● Connect to a service on a remote computer

Computer name:

☑ Login as current user

Username:

Password:

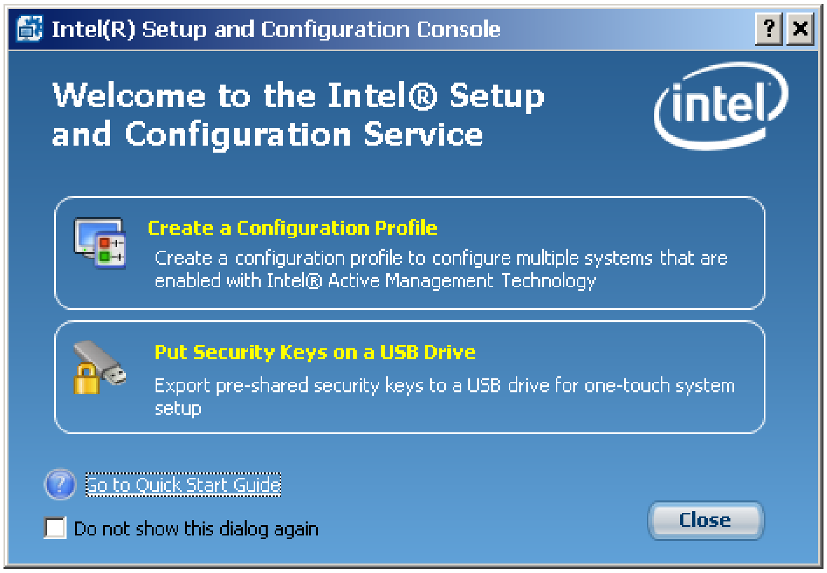
Figure 15. Connect to Service Window

2. Select one of the following:

   - **Connect to a service running on this computer** — If you start the Console on a computer running the Service, the Console automatically performs login and the Connect to Service window does not appear. If the Service you want to connect to is installed on this computer, ensure that the Service is running and then select this option.
   - **Connect to a service on a remote computer** — Select this option if the Service runs on a different computer in the Active Directory environment. Enter the name of the computer running the Service. The Console will perform login using the current user credentials. Optionally, you can clear the **Login as current user** check box and enter credentials of a different user.

Note: The user must exist in the database.

3. Click **Login**. The Welcome window appears.



Intel(R) Setup and Configuration Console

Welcome to the Intel® Setup and Configuration Service

Create a Configuration Profile

Create a configuration profile to configure multiple systems that are enabled with Intel® Active Management Technology

Put Security Keys on a USB Drive

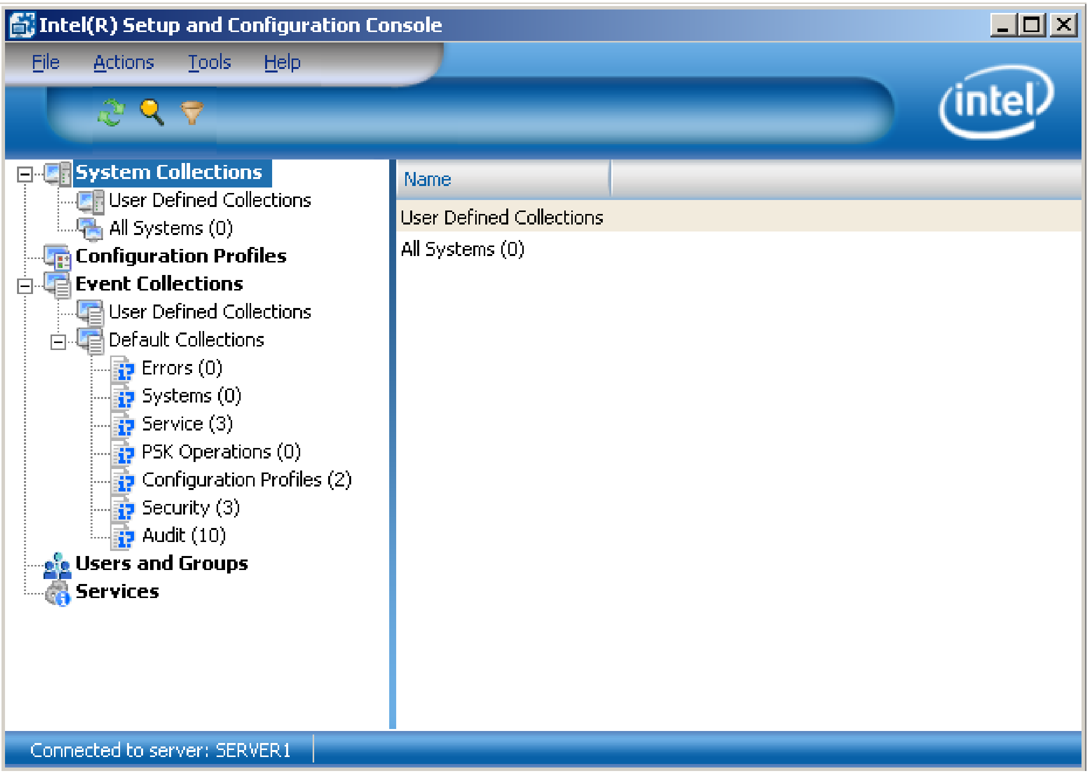
Export pre-shared security keys to a USB drive for one-touch system setup

Figure 16. Welcome Window

The Welcome window includes short-cuts to the main tasks you can perform using the Console. Note that all of the tasks are also available from the main Console window when you close the Welcome window.

You can perform the following tasks directly from the Welcome window:

- **Create a Configuration Profile** — Enables you to create a profile that defines the configuration properties for a group of Intel AMT systems. For more information, see "Defining Configuration Profiles" on page 47.
- **Put Security Keys on a USB Drive** — Enables you to generate TLS-PSK security keys for one-touch configuration of Intel AMT systems and store the keys on a USB drive. For more information, see "Configuring with TLS-PSK" on page 77.
- **Go to Quick Start Guide** — Opens the Quick Start Guide section of the context sensitive help. You can also open the help by selecting **Help** > **Help** from the main console window, or clicking **?** in the title bars of the Console wizards.
- **Close** — Closes the Welcome window and the main Console window appears.



Connected to server: SERVER1

Figure 17. Main Console Window

Note: In many of the Console screens that display lists, you can perform the following:

- Define the columns displayed in the list by right-clicking a column header and selecting the columns you want to display.
- Sort the contents of the list by double-clicking a column header.

Defining Service Settings

The following sections describe how to define Intel SCS settings:

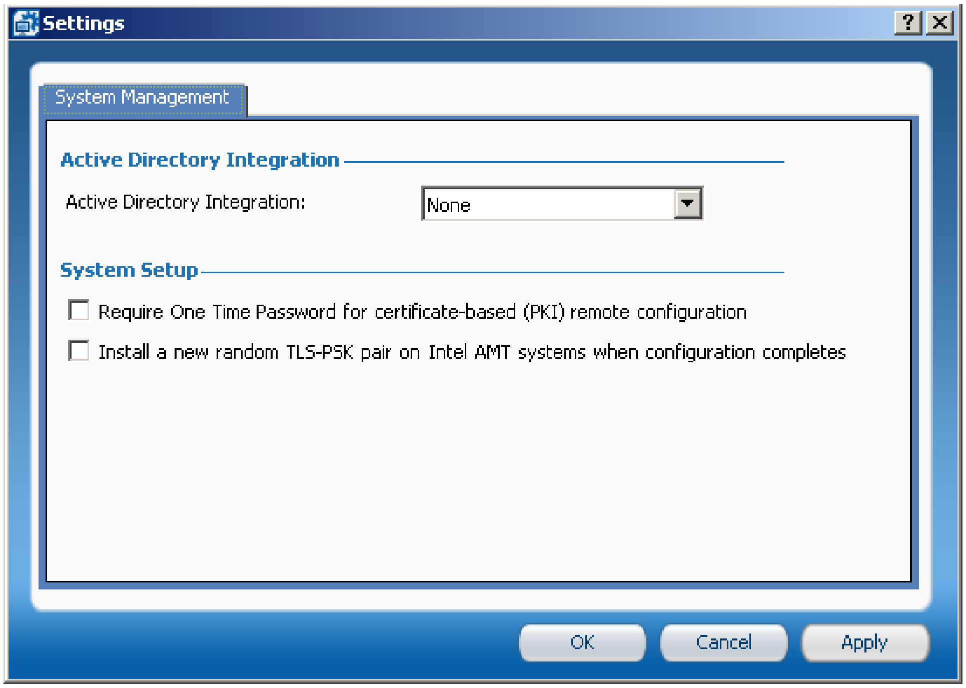
- Defining Global Service Settings
- Defining Individual Service Settings

Defining Global Service Settings

The Settings window enables you to define several global service settings.

To define global service settings:

1. Select **Tools** > **Settings**. The Settings window appears.



Active Directory Integration

Active Directory Integration: None

System Setup

□ Require One Time Password for certificate-based (PKI) remote configuration

□ Install a new random TLS-PSK pair on Intel AMT systems when configuration completes

Figure 18. Settings Window

2. From the Active Directory Integration drop-down list, select one of the following:
   - **Standard** — Integrate with Active Directory (see “Integration with Active Directory” on page 4).
   - **None** — No integration with Active Directory.
   - **Schema Extension** — This option is for backward compatibility with previous versions of the Intel SCS that included an option to extend the Active Directory schema by adding a new class (Intel-Management-Engine), based on the computer object. This option appears only if a pre-version 6.0 installation using schema extension was upgraded to Intel SCS version 6.0.

Note: Changing this setting from *Schema Extension* to a different setting is NOT reversible.

3. If required, select **Require One Time Password for certificate-based (PKI) remote configuration**. If this check box is selected, when the Intel SCS performs configuration using PKI the configuration will continue only after receiving and verifying the OTP from the Intel AMT system. For more information, see “About Remote Configuration” on page 104.

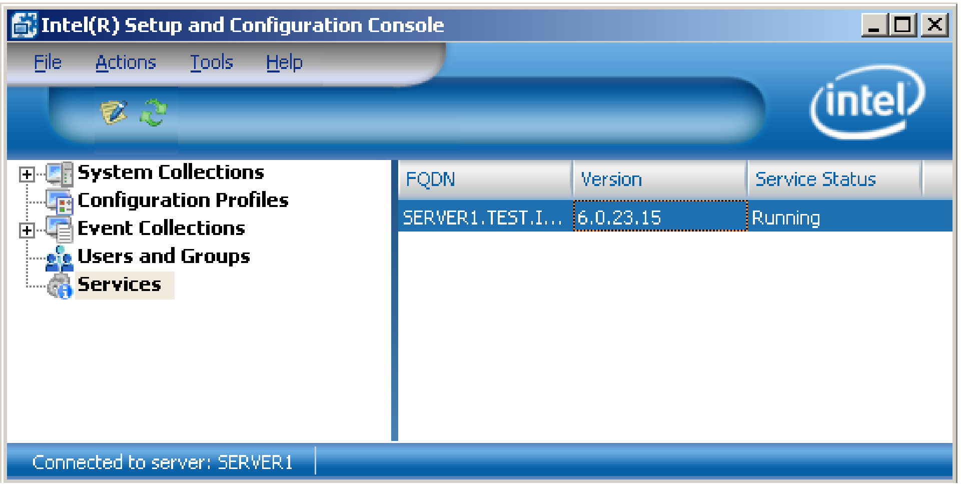
4. If required, select **Install a new random TLS-PSK pair on Intel AMT systems when configuration completes**. If this check box is selected, in the final stages of configuration the Intel SCS creates and installs a TLS-PSK pair on the Intel AMT system. After performing a reset configuration, this TLS-PSK pair is used to ensure secure communications between the system and the Intel SCS during all future configurations (even if a root certificate hash is installed on the Intel AMT system to enable TLS-PKI communication).

5. Click **OK**. The Settings window closes.

> **Note:** In a multiple Service environment, all other Services must be restarted after global service settings are changed.

Defining Individual Service Settings

All the instances of the Service that exist in the network are displayed in the *Services* node of the Console. You can view details about each Service and define different settings for each one.



FQDN	Version	Service Status
SERVER1.TEST.I...	6.0.23.15	Running

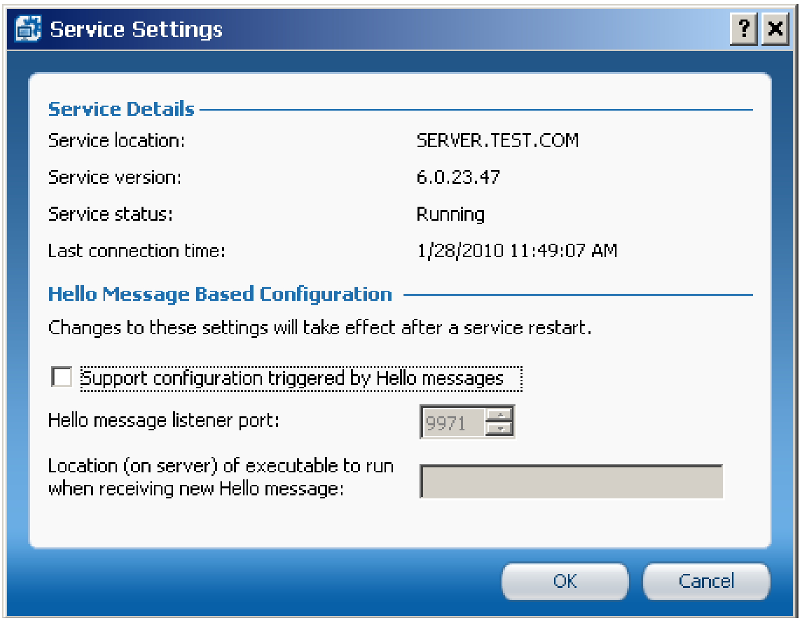
Connected to server: SERVER1

Figure 19. Service Settings Node

To define individual service settings:

1. From the Console tree select the *Services* node and perform one of the following:
   - Right-click the required service and select **Edit**
   - Select the Service, and then from the toolbar click ✎ or select **Actions** > **Edit System**

   The Service Settings window appears.



Service Settings

Service Details

Service location: SERVER.TEST.COM

Service version: 6.0.23.47

Service status: Running

Last connection time: 1/28/2010 11:49:07 AM

Hello Message Based Configuration

Changes to these settings will take effect after a service restart.

□ Support configuration triggered by Hello messages

Hello message listener port: 9971

Location (on server) of executable to run when receiving new Hello message:

Figure 20. Service Settings Window

2. If required, select **Support configuration triggered by Hello messages**. If this check box is selected, this Service will listen for “Hello” messages. If you select this check box, define the following:

   a. **Hello message listener port** — Each instance of the Service listens for “Hello” messages from Intel AMT systems on a defined TCP port. Enter the TCP port used for listening. The default port is 9971.

   b. Optionally, enter the path to a script that will provide the required information about the Intel AMT systems. If the script is located on a remote server, ensure that you define the path using the Universal Naming Convention (UNC) syntax. To use a script, the user account running the Service must:

      - Have sufficient permissions on the server where the script is located to run scripts.

      - Exist as a user in the Console with the *Edit* privilege on System configuration data (see “Creating Intel SCS Users” on page 43).

Note:

- For more information about sending configuration requests using “Hello” messages, see “Send a Configuration Request to the Intel SCS” on page 41.

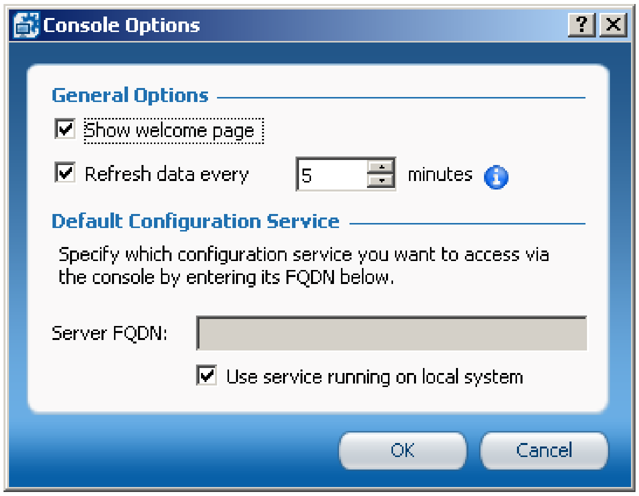
- The *Sample_Configuration_Scripts* folder in the installation package includes sample scripts and a *Scripts Description.txt* file that describes how to use scripts with the Intel SCS.

Defining Console Settings

The Console Options window enables you to define several Console settings.

To view or modify the Console settings:

1. Select **Tools** > **Console Options**. The Console Options window appears.



☑ Show welcome page

☑ Refresh data every 5 minutes

Specify which configuration service you want to access via the console by entering its FQDN below.

Server FQDN:

☑ Use service running on local system

Figure 21. Console Options Window

2. In the General Options section, select the check boxes of the required settings:
   - **Show welcome page** — Show the Welcome page when the Console is opened.
   - **Refresh data every x minutes** — Selecting this check box causes the data displayed in the Console to be updated automatically. Type or select the number of minutes in the refresh interval field. If automatic refresh is not enabled, the data is updated every time a window is displayed (entered) by the user.
3. The Server FQDN field contains the FQDN of the server where the Service is installed. (If the Console is installed on the same computer as the Service, then the field is empty and the Use service running on local system check box is selected.) If you have installed multiple instances of the Service in your environment, then you can define which instance of the Service this Console will connect to by editing the Server FQDN field entry. When you change the entry, the Console immediately tries to connect to the Service according to the new FQDN.
4. Click **OK**. The Console Options window closes.

Configuring an Intel AMT System

To configure an Intel AMT system you use a combination of the Console, the Service, and the Activator utility, as described in the following steps.

1. Define Configuration Profiles

The Intel SCS performs setup and configuration of Intel AMT systems using the parameters you define in configuration profiles.

For more information, see “Defining Configuration Profiles” on page 47.

2. Define User Privileges in the Intel SCS

If you want to enable other users to perform actions from the Console or via the API, you must define them, and their privileges, in the database.

For more information, see “About Intel SCS Users” on page 42.

3. Prepare for Configuration

How you perform this task depends on several parameters, described in “Transport Layer Security Protocol” on page 3.

- If you intend to use TLS-PSK during configuration:
    - If the OEM has installed the configuration keys on the Intel AMT system, import the keys from the file that the OEM sent you.

      For more information, see “Importing Configuration Keys from a File” on page 78.
    - If you need to create and install the configuration keys yourself, create configuration keys in the database and install them on the Intel AMT systems using one of the following methods:
        - “Creating and Exporting Configuration Keys to a USB Drive” on page 78
        - “Creating and Printing Configuration Keys” on page 80
- If you intend to use PKI during configuration, install a client certificate on the computer running the Service.

  For more information, see “Remote Configuration” on page 104.

4. Send a Configuration Request to the Intel SCS

The Intel SCS requires identification information for each Intel AMT system before it can perform the setup and configuration. How this information is entered into the database depends on which of the following methods is used to send configuration requests:

- Activator Configuration Requests — Use the Activator utility to create and send the configuration request from the Intel AMT system to the Intel SCS. The configuration requests contain all the information that the Intel SCS requires. When the request arrives, the system is automatically added to the database and configuration is performed. This is the method that Intel recommends.

  For more information, see the *Intel vPro Technology Activator Utility Release Notes and User Guide*

- “Hello” Messages — A Hello message contains the UUID of the Intel AMT system. When a Hello message arrives, the Intel SCS searches for the UUID in the database. If the system has been manually added to the database, the Intel SCS configures the system with the configuration profile defined in the database record. If the UUID does not exist in the database, the Intel SCS checks if a script has been defined to provide the required information about the Intel AMT system. If a script exists, it is performed and the system is added to the database and configuration is performed. If a script does not exist, a record for the system is added to the database with a status of *Missing Configuration Data*.

  Hello messages can be sent to the Intel SCS in the following ways:

  - If an Intel AMT system has been prepared by the OEM to use the “Bare Metal” feature of Remote Configuration, it will start to send “Hello” messages as soon as it is connected to AC power.
  - You can use the Activator CLI to send a “Hello” message from the Intel AMT system.

  Using the Hello messages option requires the following:

  - The Service must be defined to listen for “Hello” messages as described in “Defining Individual Service Settings” on page 37.
  - The initial conditions described in “Prerequisites for Remote Configuration” on page 105.
  - To use a script, the user account running the Service must be added to the Console as a user with the *Edit* privilege on System configuration data.
  - To add a system to the database, from the Console tree right-click **All Systems** and select **Add System Definition**.

5. Verify that the Intel AMT System is Configured

Ensure that the Intel SCS successfully configured the Intel AMT system.

For more information, see “Viewing and Editing Intel AMT Systems” on page 82

When the Intel SCS has successfully configured the Intel AMT system, you can perform tasks directly from your management console.

4

Defining Users in the Intel SCS

This chapter describes how to define users in the Intel SCS.

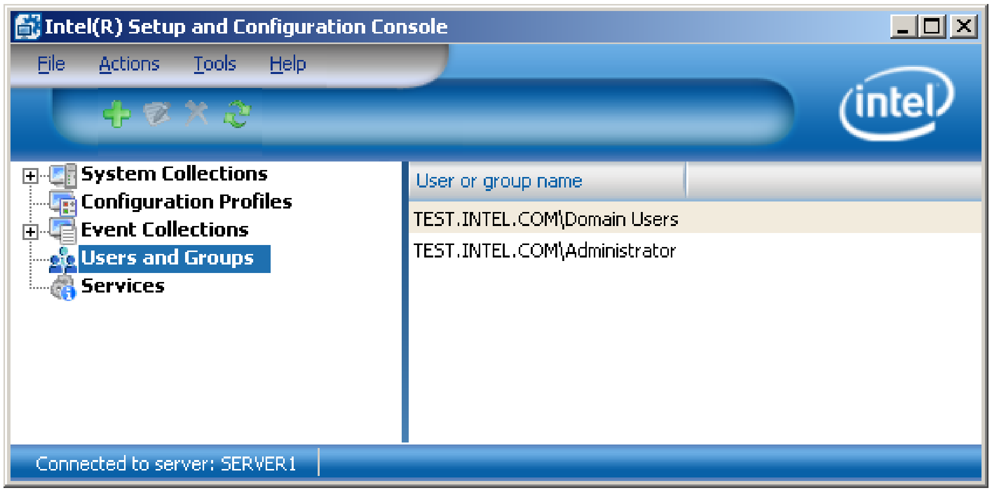
It includes the following topics:

- About Intel SCS Users
- Creating Intel SCS Users
- User Tasks and Privileges

About Intel SCS Users

All actions that a user can perform in the Intel SCS are controlled by privileges that you grant to the user. When a user logs into the Console, or tries to perform an action via the API, he can only perform an action if he has the correct privileges (see "User Tasks and Privileges" on page 45).

The users and user groups are displayed in the *Users and Groups* node of the Console tree.



TEST.INTEL.COM\Domain Users
TEST.INTEL.COM\Administrator

Figure 22. Users and Groups Node

The following table describes the actions you can perform from the Users and Groups node.

Table 6. Users and Groups Node Actions

Action	How to...
Create an Intel SCS user	See "Creating Intel SCS Users" on page 43
Edit the privileges of an existing user/group	Select the user/group and then perform one of the following: • Right-click and select **Edit** • From the toolbar, click ✎ or select **Actions** > **Edit**
Delete an existing user/group	Select the user/group and then perform one of the following: • Right-click and select **Delete** • From the toolbar, click ✖ or select **Actions** > **Delete** (You can not delete the user with which you are currently logged into the Console.)
Refresh the displayed list of users/groups	• Right-click **Users and Groups** and select **Refresh** • From the toolbar, click ⟳

Creating Intel SCS Users

The Console enables you to select users or groups from the Active Directory, grant them privileges, and save the details in the database. If you grant privileges to a user and a user group that the user belongs to, the user will have the privileges according to the highest privilege of the user or group.

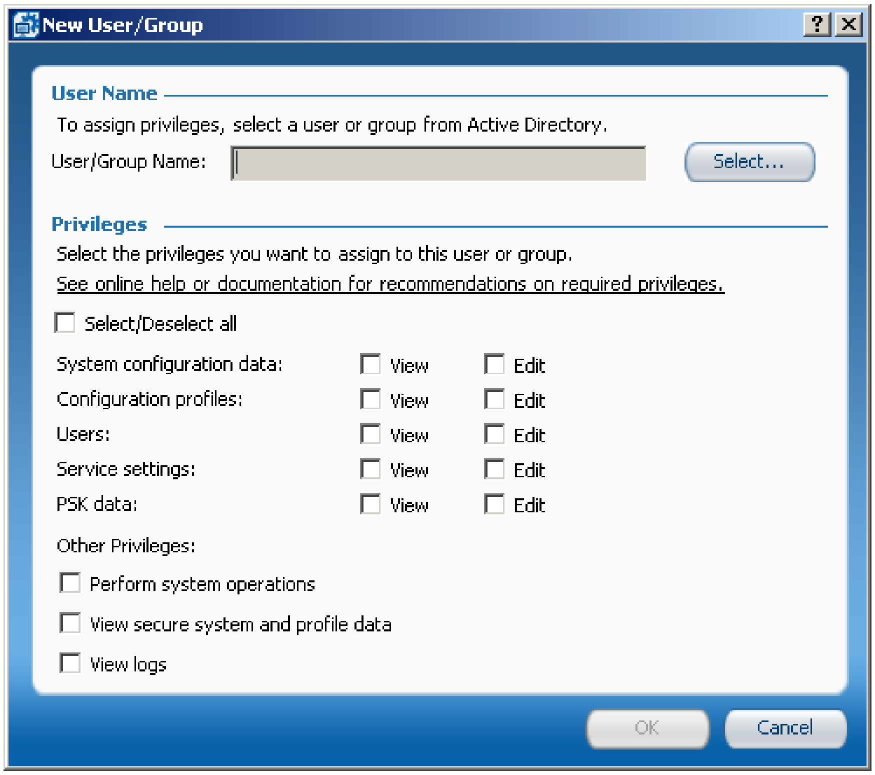
For information about which privileges are required to perform common tasks in the Intel SCS, see "User Tasks and Privileges" on page 45.

Note: If you add/remove users or change privileges of an existing user, you must close and then re-open all the Consoles in the network for the changes to be implemented successfully.

To create a User/Group:

1. From the Console tree, select **Users and Groups** and perform one of the following:
   - Right-click and select **Add**
   - From the toolbar, click ✚ or select **Actions** > **Add**

The New User/Group window appears.



User Name

To assign privileges, select a user or group from Active Directory.

User/Group Name:

Privileges

Select the privileges you want to assign to this user or group.

See online help or documentation for recommendations on required privileges.

□ Select/Deselect all

System configuration data: □ View □ Edit

Configuration profiles: □ View □ Edit

Users: □ View □ Edit

Service settings: □ View □ Edit

PSK data: □ View □ Edit

Other Privileges:

□ Perform system operations

□ View secure system and profile data

□ View logs

Figure 23. New User/Group Window

2. Click **Select** to browse and select the user or group from the Active Directory.

3. From the list of privileges, select the check boxes of the privileges that you want to give to this user/group, as described in the following table.

Table 7. Privileges

Privilege	**Description**
System configuration data	• View — View information about the Intel AMT systems • Edit — Change configuration settings of systems, perform configuration operations, add and delete systems from the database
Configuration profiles	• View — View the settings in configuration profiles (not including passwords) • Edit — Create, edit, and delete configuration profiles
Users	• View — View the users and their resource privileges • Edit — Add new users, edit the privileges of existing users, and delete users
Service settings	• View — View the settings of the Intel SCS • Edit — Edit the settings of the Intel SCS

Table 7. Privileges (Continued)

Privilege	Description
PSK data	• View — View the list of TLS-PSK keys • Edit — Allows the user to create new TLS-PSK keys, and import TLS PSK keys to the database
Perform system operations	Test the connectivity between the Intel SCS and Intel AMT systems
View secure system and profile data	View passwords
View logs	View the Intel SCS log records

4. Click **OK**. The New User/Group window closes and the new user/group is added to the list of users and groups.

User Tasks and Privileges

The following table describes common tasks and the privileges you need to assign to users that need to perform them.

Table 8. Tasks and Privileges

Task	Required/Recommended Privileges
Use the Activator CLI	**Required**: • System configuration data (View and Edit) • PSK data (View and Edit)
Use the Activator GUI	**Required**: • System configuration data (View and Edit) • PSK data (View and Edit) • Configuration profiles (View)
Create and Modify Configuration Profiles	**Required**: • Configuration profiles (View and Edit) • View secure system and profile data **Recommended**: • Service settings (View and Edit) • View logs

Table 8. Tasks and Privileges

Task	Required/Recommended Privileges
Modify Intel AMT System's Configuration Data	**Required**: • System configuration data (View and Edit) • View profiles **Recommended**: • View secure system and profile data • View logs • Perform system operations
Create USB Key	**Required**: PSK data (View and Edit) **Recommended**: View logs
Manage Intel SCS Users	**Required**: Users (View and Edit) **Recommended**: View logs
Run a script to process "Hello" messages	The user account running the Service (*SCSServer.exe*) requires View and Edit privileges on System configuration data. For more information about running scripts, see "Send a Configuration Request to the Intel SCS" on page 41.

5

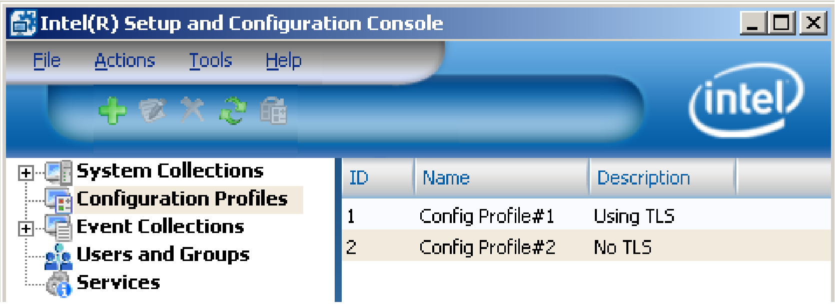
Defining Configuration Profiles

This chapter describes how to define configuration profiles. It includes the following topics:

- About Configuration Profiles
- Creating a Configuration Profile
- Defining the Access Control List (ACL) in the Profile
- Defining Domains in the Profile
- Defining Remote Access in the Profile
- Defining the Trusted Root Certificates
- Defining Common Names in the Certificate Subject Name
- Defining Transport Layer Security (TLS) in the Profile
- Defining Network Setups in the Profile
- Defining System Settings in the Profile
- Viewing Profile History

About Configuration Profiles

A configuration profile enables you to configure multiple Intel AMT systems with the same set of configuration properties. You can create several profiles with different settings and select from the profiles when you want to configure the systems. The Console includes a wizard that you use to create and modify the profiles. The profiles you create are displayed in the *Configuration Profiles* node of the Console tree.



ID	Name	Description
1	Config Profile#1	Using TLS
2	Config Profile#2	No TLS

Figure 24. Configuration Profiles Node

The following table describes the actions you can perform from the Configuration Profiles node.

Table 9. Configuration Profiles Node Actions

Action	**How to...**
Create a new configuration profile	See "Creating a Configuration Profile" **on page 49**
Edit an existing profile	Select the profile and then perform one of the following: • Right-click and select **Edit Profile** • From the toolbar, click or select **Actions** > **Edit Profile**
Delete an existing profile	Select the profile and then perform one of the following: • Right-click and select **Delete Profile** • From the toolbar, click or select **Actions** > **Delete Profile** (You can not delete a profile if an Intel AMT system is configured with it.)
Create a copy of an existing profile	Select the profile and then perform one of the following: • Right-click and select **Clone Profile** • From the toolbar, click or select **Actions** > **Clone Profile** You can then edit specific settings that you want to change.
View profile details and history	See "Viewing Profile History" on page 76
Refresh the displayed list of profiles	From the Console tree, select **Configuration Profiles** and perform one of the following: • Right-click and select **Refresh Profiles** • From the toolbar, click or select **Actions** > **Refresh Profiles**

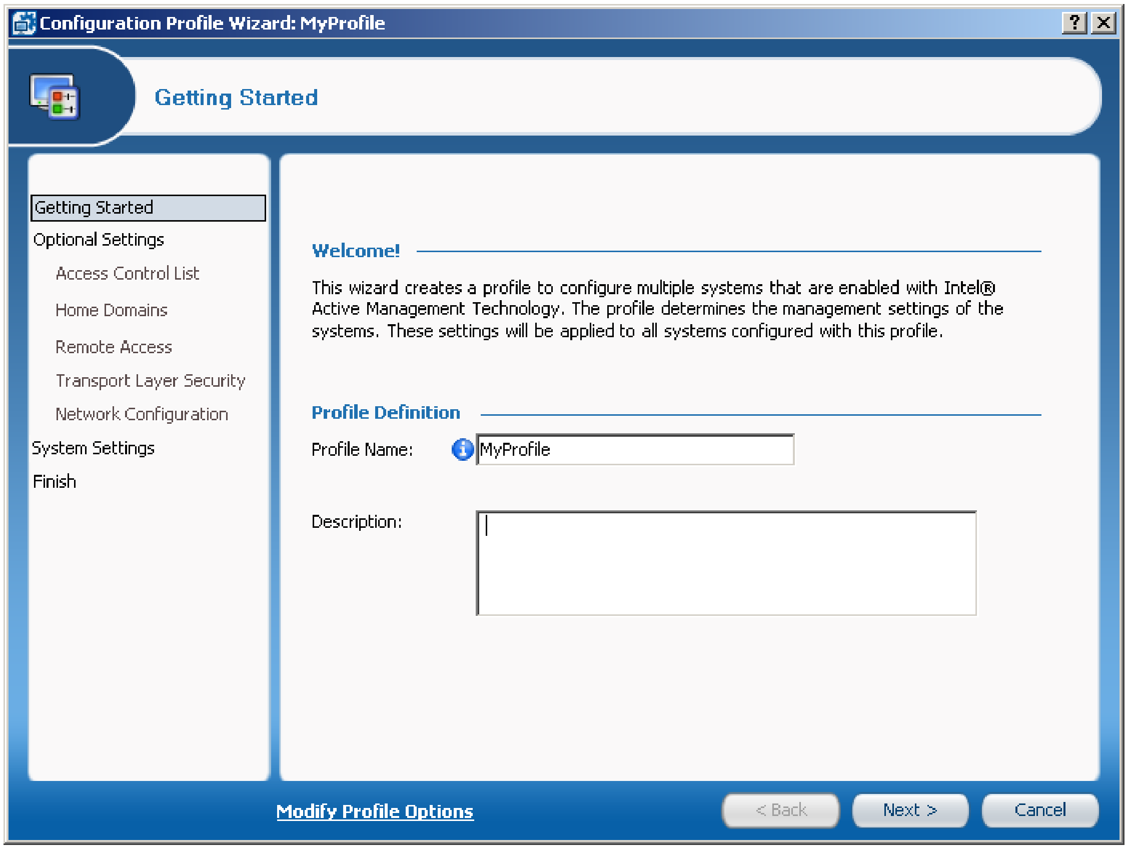
Creating a Configuration Profile

The following procedure describes how to create a configuration profile.

To create a configuration profile:

1. From the Console tree, select **Configuration Profiles** and perform one of the following:
   - Right-click and select **Add Profile**
   - From the toolbar, click ➕ or select **Actions** > **Add Profile**

   The Getting Started window of the Configuration Profile Wizard appears.



Welcome!

This wizard creates a profile to configure multiple systems that are enabled with Intel® Active Management Technology. The profile determines the management settings of the systems. These settings will be applied to all systems configured with this profile.

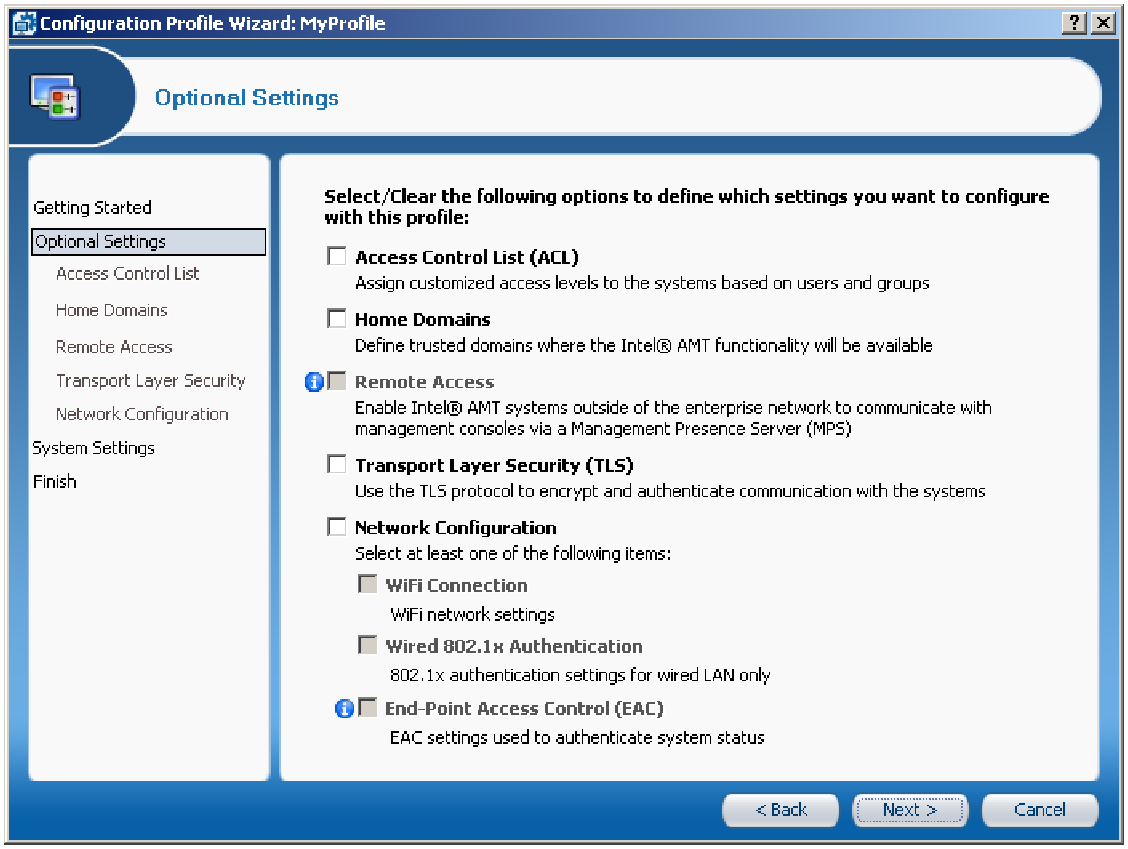
Profile Definition

Profile Name: MyProfile

Description:

Figure 25. Getting Started Window

2. In the Profile Definition section, enter a name and description for the profile or leave the default values. The profile name must be unique.
3. Click **Next**. The Optional Settings window appears. Select the check boxes of the optional settings you want to configure in this profile, and clear the check boxes of the options that you want to remove from the profile.



Select/Clear the following options to define which settings you want to configure with this profile:

□ **Access Control List (ACL)**
Assign customized access levels to the systems based on users and groups

□ **Home Domains**
Define trusted domains where the Intel® AMT functionality will be available

□ **Remote Access**
Enable Intel® AMT systems outside of the enterprise network to communicate with management consoles via a Management Presence Server (MPS)

□ **Transport Layer Security (TLS)**
Use the TLS protocol to encrypt and authenticate communication with the systems

□ **Network Configuration**
Select at least one of the following items:

□ **WiFi Connection**
WiFi network settings

□ **Wired 802.1x Authentication**
802.1x authentication settings for wired LAN only

□ **End-Point Access Control (EAC)**
EAC settings used to authenticate system status

Figure 26. Optional Settings Window

4. After selecting the required options, click **Next** to continue in the Configuration Profile Wizard and configure the settings, as described in the following sections:

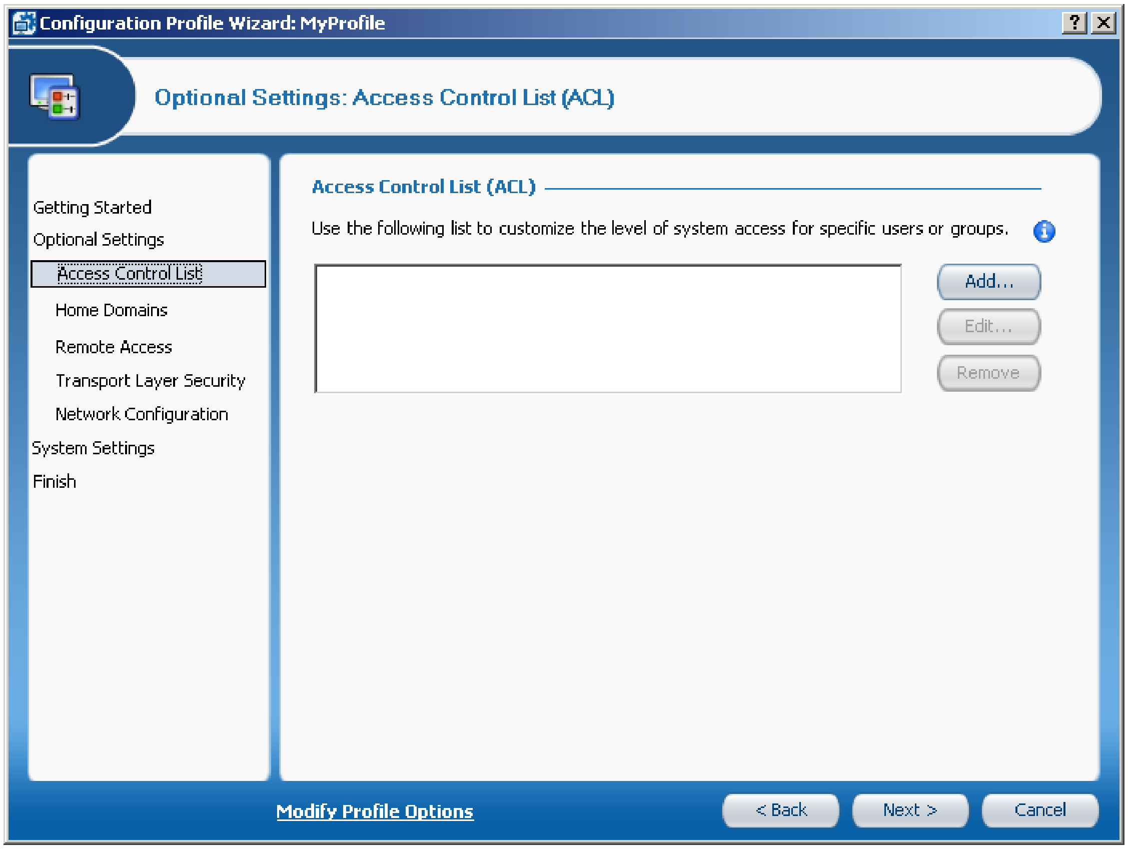
   - **Access Control List (ACL)** — See “Defining the Access Control List (ACL) in the Profile” on page 51.
   - **Home Domains** — See “Defining Domains in the Profile” on page 55.
   - **Remote Access** — See “Defining Remote Access in the Profile” on page 56.
   - **Transport Layer Security (TLS)** — See “Defining Transport Layer Security (TLS) in the Profile” on page 63.
   - **Network Configuration** — If you select this check box, you must select at least one of the following check boxes:
     - **WiFi Connection** — To define WiFi setups (including 802.1x).
     - **Wired 802.1x Authentication** — To define an 802.1x wired setup.
     - **End-Point Access Control (EAC)** — To define EAC settings.

     See “Defining Network Setups in the Profile” on page 66.
   - **System Settings** — See “Defining System Settings in the Profile” on page 72.

5. When you have completed the configuration, click **Finish**. The Configuration Profile Wizard closes and the new profile is added to the list of profiles.

Defining the Access Control List (ACL) in the Profile

The Access Control List (ACL) window of the Configuration Profile Wizard enables you to define users and their access privileges on the Intel AMT system. User identification and realm selection must be coordinated with the requirements and instructions of third-party management consoles.



Configuration Profile Wizard: MyProfile

Optional Settings: Access Control List (ACL)

Access Control List (ACL)

Use the following list to customize the level of system access for specific users or groups.

Figure 27. Access Control List (ACL) Window

You can perform the following to define the users in the ACL:

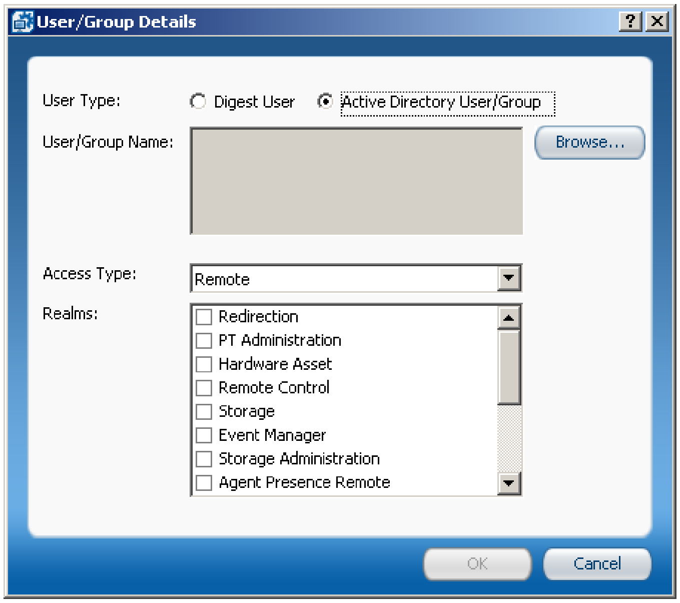
- Create a new user by clicking **Add** — See "Adding a User to the ACL" on page 52.
- Edit an existing user by clicking **Edit**.
- Remove a user from the list by clicking **Remove**.

Adding a User to the ACL

The User/Group Details window enables you to add a new user or group to the profile's Access Control List.

To add a user:

1. From the Access Control List (ACL) window, click **Add**. The User/Group Details window appears.



User/Group Details

User Type: ○ Digest User ● Active Directory User/Group

User/Group Name:

Access Type: Remote

Realms:
□ Redirection
□ PT Administration
□ Hardware Asset
□ Remote Control
□ Storage
□ Event Manager
□ Storage Administration
□ Agent Presence Remote

Figure 28. User/Group Details Window

2. In the User Type section, select the required type of user:

   - **Digest User** — When selected, the User/Group name field is replaced with a User name and password field. Enter the user name and password. Note that you can only enter seven users in a profile, even though certain Intel AMT versions support more than seven users.
   - **Active Directory User/Group** — Click … to browse and select the user or group. This option is available only if the Intel SCS is configured to work in Active Directory Integrated mode (see "Defining Service Settings" on page 36).

   Note: You can not select the default user groups from the Active Directory *Builtin* folder. Instead, either add the required users individually or create and add a new group containing the users.

3. From the Access Type drop-down list, specify an access type. This parameter defines the locations from where the user is allowed to perform an action. A user might be limited to local actions or might also be able to perform actions from the network. Select one of the following:

   - **Local** — The user can access the Intel AMT system 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).

4. From the Realms section, select the check boxes of the realms that you want to make available to this user. The realms define specific functional capabilities, such as Redirection or PT Administration, as described in the following table.

   Note that not all realms are available on all versions of Intel AMT. The Realms displayed depend on the Access Type you selected.

Table 10. Intel AMT Realms

Realm	**Capabilities**
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 Intel AMT system
Remote Control	Enables powering a system 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
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)

Table 10. Intel AMT Realms (Continued)

Realm	Capabilities
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
Local User Notification	Provides alerts to a user on the local interface
Endpoint Access Control	Returns settings associated with NAC posture
Endpoint Access Control Administrator	Configures and enables the NAC posture
Event Log Reader	Allows definition of a user with privileges only to read the Intel AMT system log
Access Monitor	Allows a system auditor to monitor all events. Before assigning this realm, see "Using Access Monitor" on page 54.
User Access Control	Groups several ACL management commands into a separate realm to enable users to manage their own passwords without requiring administrator privileges

Using Access Monitor

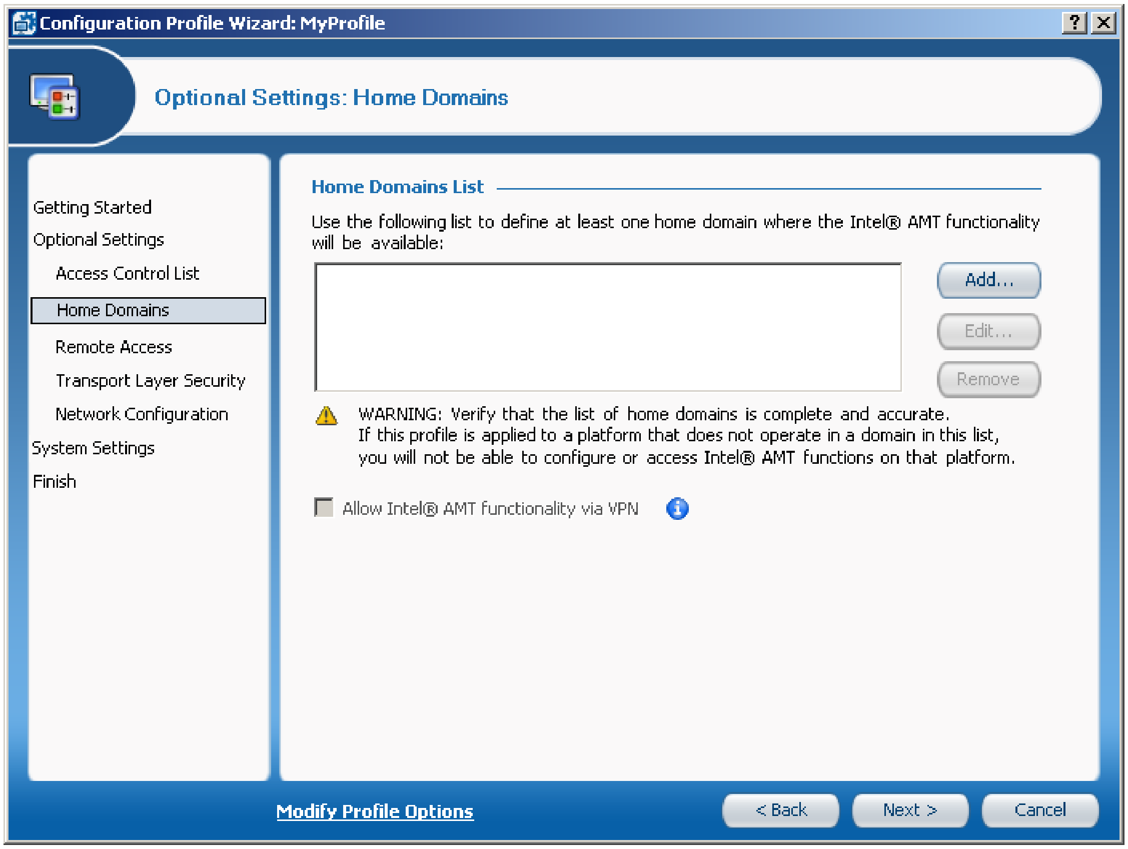
The access monitor serves as a deterrent to rogue administrator activity by tracing any attempts to perform damaging actions. The feature is implemented by means of two elements: an Audit Log and a special Auditor user that you assign the Access Monitor realm. The Intel AMT system writes selected events to the Audit Log that is accessible only to the Auditor. Only the Auditor can define which events the Intel AMT system writes to the Audit Log.

You can assign the Access Monitor realm to one user only, and only that user can then relinquish it. By default, the default *admin* user account has access to this realm.

Note: The Access Monitor feature is available from Intel AMT Release 4.0 and later.

Defining Domains in the Profile

The Home Domains window of the Configuration Profile Wizard enables you to define a list of domains where the Intel AMT system is permitted to operate.



Use the following list to define at least one home domain where the Intel® AMT functionality will be available:

WARNING: Verify that the list of home domains is complete and accurate. If this profile is applied to a platform that does not operate in a domain in this list, you will not be able to configure or access Intel® AMT functions on that platform.

□ Allow Intel® AMT functionality via VPN

Figure 29. Home Domains Window

To define the domains:

1. Click **Add**. The Domain Properties window appears.
2. Enter the DNS suffix name and click **OK**. The Domain Properties window closes and the domain appears in the list of domains.

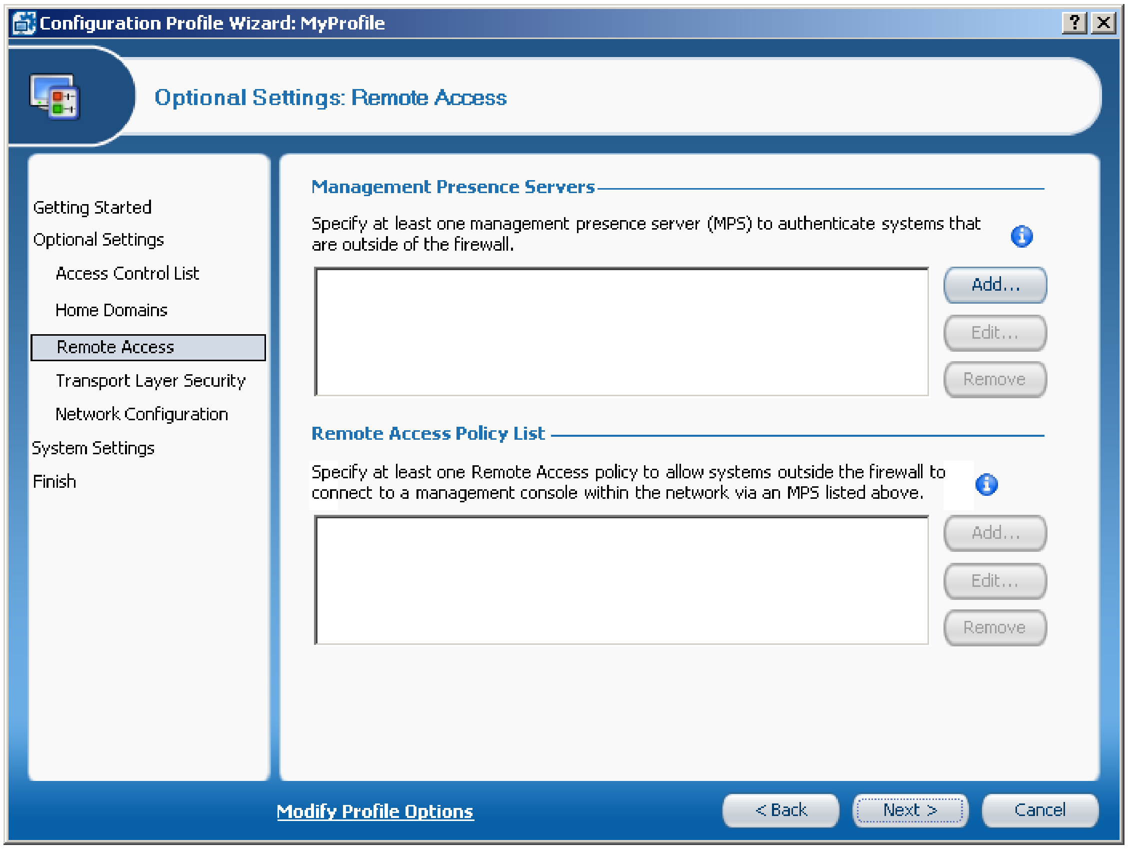
Note: Ensure that the list of home domains is complete and accurate. If this profile is applied to an Intel AMT system that does not operate in a domain in this list, you will not be able to configure or access Intel AMT functions on that system.

3. Optionally, select **Allow Intel® AMT functionality via VPN**. This configures Intel AMT systems to accept management traffic over a Virtual Private Network connection when Intel AMT detects that the system is operating outside the enterprise network.

Defining Remote Access in the Profile

Intel AMT Release 4.x and later releases include a remote access feature which enables Intel AMT systems located outside an enterprise to connect to management consoles inside the enterprise network. 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 remote access to work, the Intel AMT system must first be configured by the Intel SCS when it is inside the enterprise with the information needed to connect with the MPS.



Specify at least one management presence server (MPS) to authenticate systems that are outside of the firewall.

Specify at least one Remote Access policy to allow systems outside the firewall to connect to a management console within the network via an MPS listed above.

Figure 30. Remote Access Window

To define the remote access parameters, see the following:

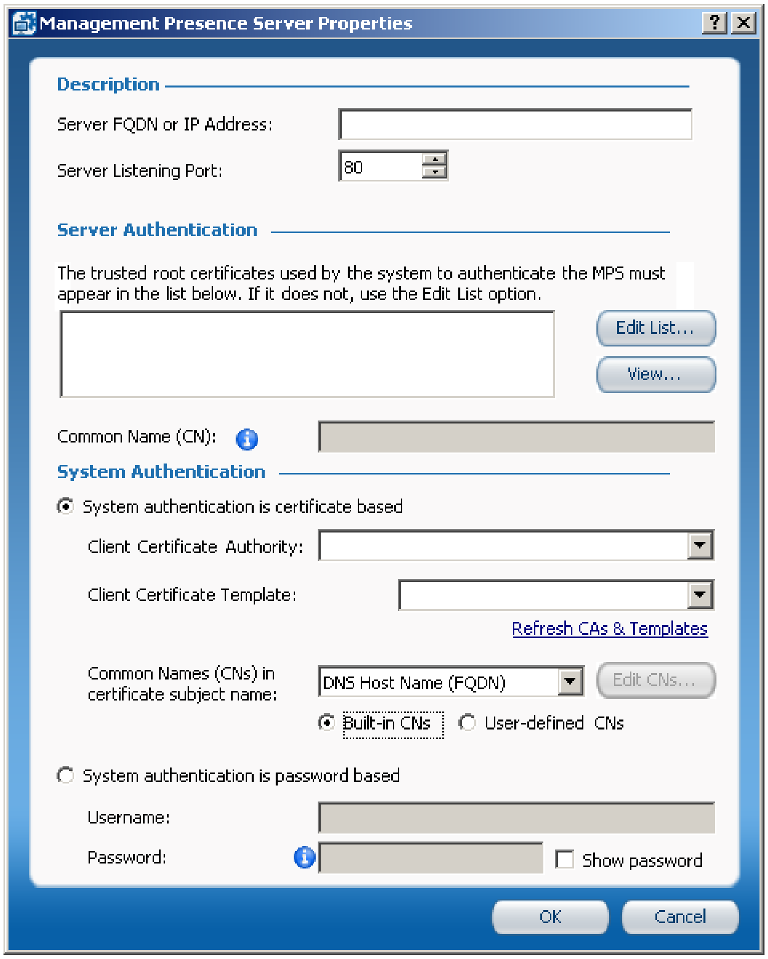
- “Defining Management Presence Servers” on page 57.
- “Defining Remote Access Policies” on page 58.

Defining Management Presence Servers

You can define up to four Management Presence Servers in a configuration profile.

To define a management presence server:

1. From the Management Presence Servers section of the Remote Access window, click **Add**. The Management Presence Server Properties window appears.



Management Presence Server Properties

Description

Server FQDN or IP Address:

Server Listening Port: 80

Server Authentication

The trusted root certificates used by the system to authenticate the MPS must appear in the list below. If it does not, use the Edit List option.

Common Name (CN):

System Authentication

● System authentication is certificate based

Client Certificate Authority:

Client Certificate Template:

Common Names (CNs) in certificate subject name: DNS Host Name (FQDN)

● Built-in CNs ○ User-defined CNs

○ System authentication is password based

Username:

Password:

□ Show password

Figure 31. Management Presence Server Properties Window

2. In the Server FQDN or IP Address field, enter the FQDN or IP address of the Management Presence Server.

3. In the Server Listening Port field, enter the Port that the Management Presence Server listens on for connections from Intel AMT systems.

4. Define the trusted root certificates that will be used by Intel AMT systems configured with this profile (see “Defining the Trusted Root Certificates” on page 59).

5. If you entered an IP address in the Server FQDN or IP Address field, 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.)

6. To define authentication based on certificates, select **System authentication is certificate based** and perform the following:

   a. From the Client Certificate Authority drop-down list, select the Enterprise Certificate Authority that the Intel AMT system will use to request a certificate that the MPS can authenticate.

   b. From the Client Certificate Template drop-down list, select a template defined for creating the appropriate client certificate. The available templates will be templates where the Subject Name is supplied in the request and the usage is “Client Authentication” (see “Certification Authorities and Templates” on page 113).

   c. Define the Common Names that will be included in the Subject Name of the generated certificate (see “Defining Common Names in the Certificate Subject Name” on page 61).

7. To define authentication based on a password, select **System authentication is password based** and enter a user name and password.

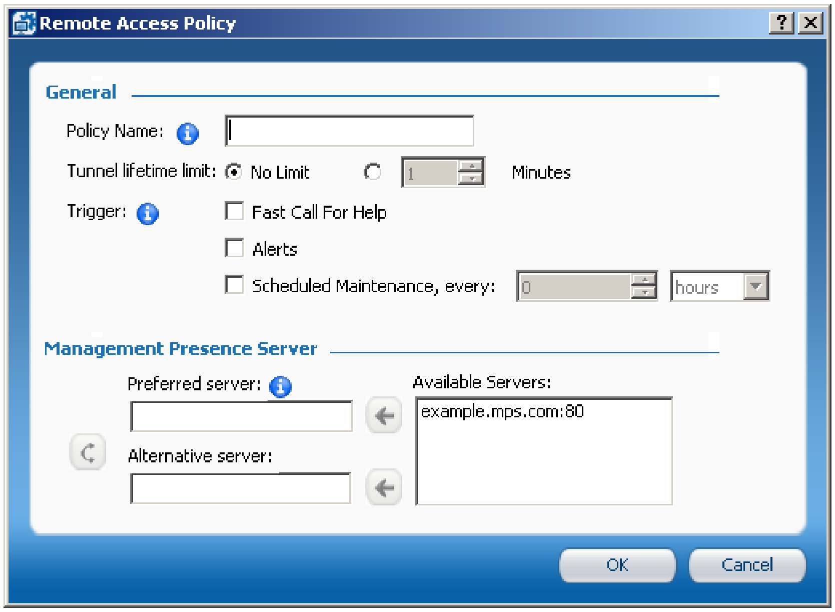
8. Click **OK**. The settings are saved and the Management Presence Server window closes.

Defining Remote Access Policies

A Remote Access policy determines the conditions (triggers) for establishing an MPS connection, and to which MPS to connect. You must define at least one Remote Access policy.

To define a remote access policy:

1. From the Remote Access Policy List section of the Remote Access window, click **Add**. The Remote Access Policy window appears.



Remote Access Policy

General

Policy Name:

Tunnel lifetime limit: ● No Limit ○ 1 Minutes

Trigger:
□ Fast Call For Help
□ Alerts
□ Scheduled Maintenance, every: 0 hours

Management Presence Server

Preferred server:

Alternative server:

Available Servers:
example.mps.com:80

Figure 32. Remote Access Policy Window

2. In the Policy Name field, enter a descriptive name for the policy.
3. In the Tunnel lifetime limit field, enter an interval in minutes. When there is no activity in an established tunnel for this period of time, the Intel AMT device will close the tunnel. Selecting **No Limit** means the tunnel will not time out but will stay open until it is closed by the user or when a different policy with higher priority needs to be processed.
4. In the Trigger section, select the trigger or triggers associated with this policy:
   - **Fast Call For Help** — The Intel AMT device establishes a tunnel with the MPS when the user initiates a connection request.
   - **Alerts** — The device establishes a connection when an event occurs that generates an alert addressed to the network interface.
   - **Scheduled Maintenance, every** — The device connects to the MPS based on the number of hours, minutes, or seconds defined here.

   Note: A policy can include one or more triggers, but no two policies can contain the same trigger.

5. In the Management Presence Server section, 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.
6. Click **OK**. The Remote Access Policy window closes.

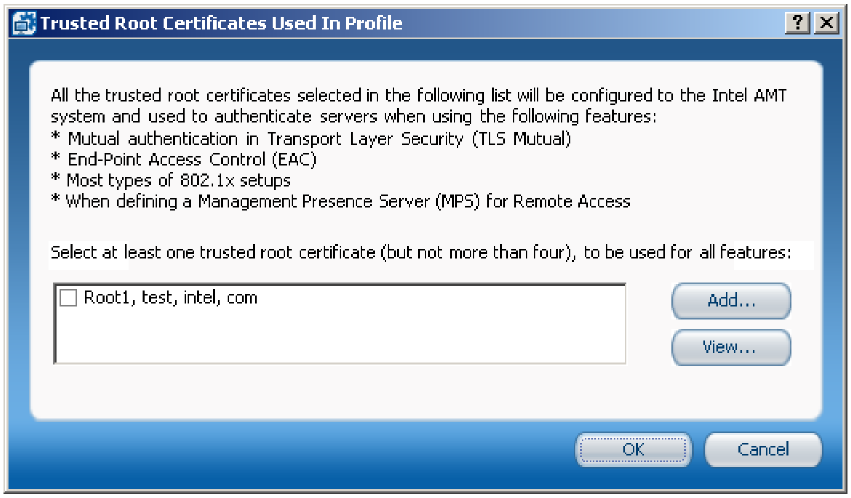
Defining the Trusted Root Certificates

The following procedure describes how to define which trusted root certificates Intel AMT systems configured with this profile will use with the following features:

- When defining a Management Presence Server
- Mutual authentication in Transport Layer Security
- Most types of 802.1x setups
- End-Point Access Control

To define the trusted root certificates:

1. From the relevant feature window, click **Edit List**. The Trusted Root Certificates Used In Profile window appears.



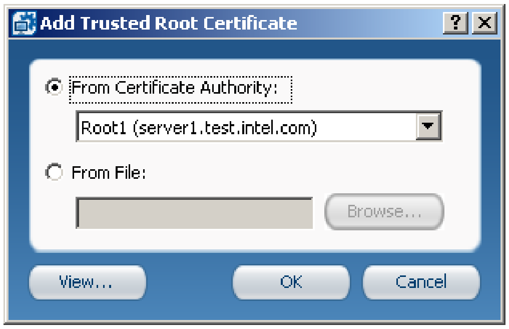
All the trusted root certificates selected in the following list will be configured to the Intel AMT system and used to authenticate servers when using the following features:
* Mutual authentication in Transport Layer Security (TLS Mutual)
* End-Point Access Control (EAC)
* Most types of 802.1x setups
* When defining a Management Presence Server (MPS) for Remote Access

Select at least one trusted root certificate (but not more than four), to be used for all features:

□ Root1, test, intel, com

Figure 33. Trusted Root Certificates Used In Profile

2. To add a trusted root certificate, click **Add**. The Add Trusted Root Certificate window appears



● From Certificate Authority:

Root1 (server1.test.intel.com)

○ From File:

Figure 34. Add Trusted Root Certificate Window

3. Select one of the following:

   - **From Certificate Authority** — From the drop-down list select the Enterprise Certification Authority (CA).
   - **From File** — Enter the path to the file or click **Browse** to locate and select a certificate.

Note:

- You can only add a certificate from a CA if the certificate is self-signed and the CA is a root CA. You cannot add a certificate from a subordinate CA.
- You can view details of the certificate by clicking **View**.

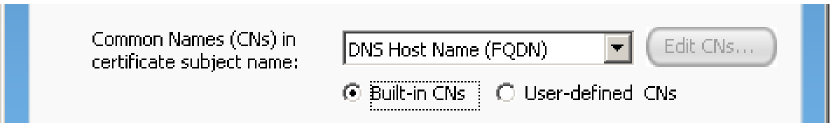
4. Click **OK**. The Add Trusted Root Certificate window closes and the certificate appears in the Trusted Root Certificates Used In Profile window.
5. Select the check box of at least one of the trusted root certificates in the list.
6. Click **OK**. The Trusted Root Certificates Used In Profile window closes.

Defining Common Names in the Certificate Subject Name

The following procedures describe how to define which Common Names (CNs) will be included in the generated certificate's Subject Name when using the following features:

- When defining a Management Presence Server
- Mutual authentication in Transport Layer Security
- Most types of 802.1x setups
- End-Point Access Control

You can use the following options to define different CNs for each of the features:



Common Names (CNs) in certificate subject name: DNS Host Name (FQDN)

● Built-in CNs ○ User-defined CNs

Figure 35. Common Name Options

Note: Due to Microsoft limitations, the Intel SCS might fail to create a certificate in the following situations:

- If the AMT's FQDN is longer than 64 characters
- If the certificate subject is longer than 256 characters
- If one of the CN types is **Distinguished Name**, and the Distinguished Name is longer than 256 characters

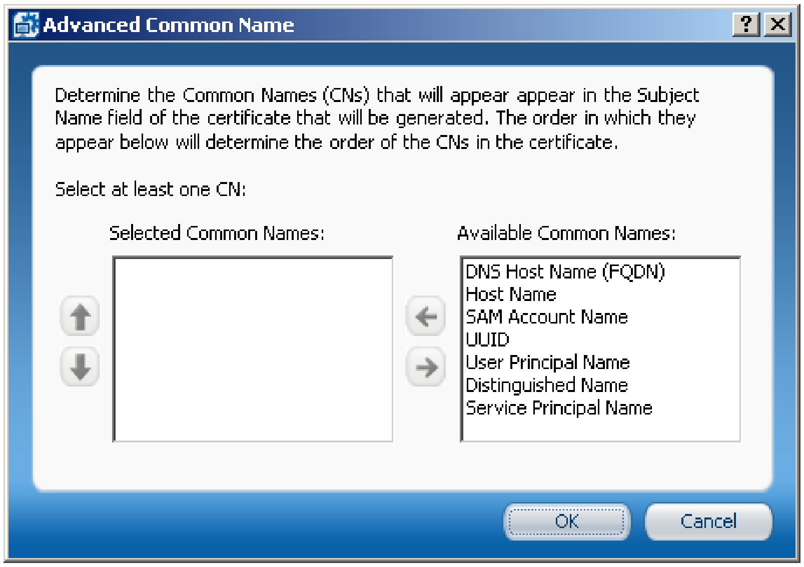
To use "built-in" common names:

1. From the relevant feature window, select **Built-in CNs**.
2. From the Common Names (CNs) in certificate subject name drop-down list, select the format that the Intel AMT device expects for the first CN in a certificate. This can be one of the following:
   - **DNS Host Name (FQDN)**— FQDN of the Intel AMT device
   - **Host Name** — Host name of the Intel AMT system (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)

   Note: The Subject Name of the generated certificate will include all three of these CNs and the Intel AMT platform's UUID.

To use user-defined common names:

1. From the relevant feature window, select **User-defined CNs**.
2. Click **Edit CNs**. The Advanced Common Name window appears.



Determine the Common Names (CNs) that will appear appear in the Subject Name field of the certificate that will be generated. The order in which they appear below will determine the order of the CNs in the certificate.

Select at least one CN:

DNS Host Name (FQDN)
Host Name
SAM Account Name
UUID
User Principal Name
Distinguished Name
Service Principal Name

Figure 36. Advanced Common Name Window

3. From the Available Common Names list, select the required CNs and click ← to add them to the Selected Common Names list. The selected CNs will appear in the certificate Subject Name according to the order that they appear in the Selected Common Names list. (Use the Up/Down arrows to change the order.)

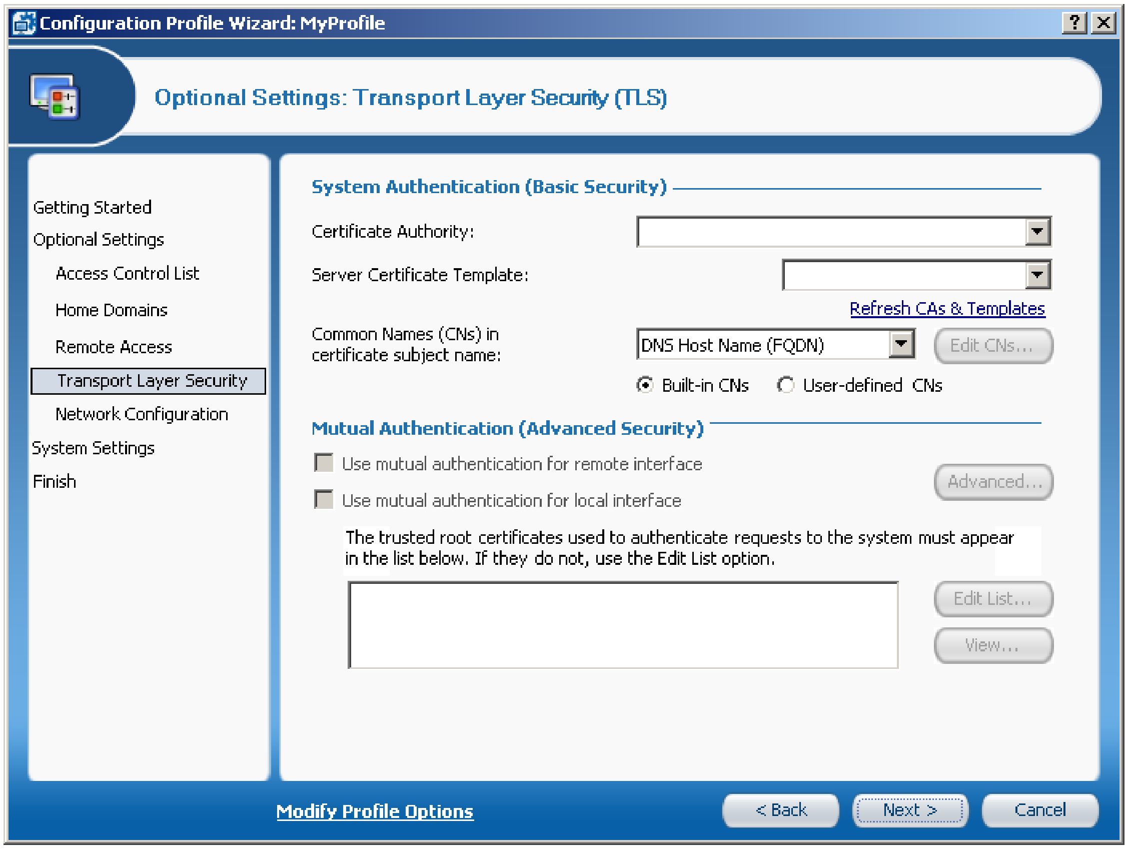
Note:

- Select the Distinguished Name CN only if you need to authenticate the Intel AMT system against an Active Directory Lightweight Directory Access Protocol (LDAP) database.
- If you select the Distinguished Name CN, do not add additional CNs since due to a Microsoft limitation the order that they appear in the certificate cannot be guaranteed.

Defining Transport Layer Security (TLS) in the Profile

The Transport Layer Security (TLS) window of the Configuration Profile Wizard enables you to define the TLS settings for the profile. When TLS is enabled, the Intel AMT device requires a server certificate to authenticate itself with other applications.

If mutual TLS authentication is enabled, any applications that interact with the device must supply client certificates that the device uses to authenticate the applications.



Configuration Profile Wizard: MyProfile

Optional Settings: Transport Layer Security (TLS)

Getting Started
Optional Settings
Access Control List
Home Domains
Remote Access
Transport Layer Security
Network Configuration
System Settings
Finish

System Authentication (Basic Security)

Certificate Authority:

Server Certificate Template:

Common Names (CNs) in certificate subject name: DNS Host Name (FQDN)

● Built-in CNs ○ User-defined CNs

Mutual Authentication (Advanced Security)

□ Use mutual authentication for remote interface

□ Use mutual authentication for local interface

The trusted root certificates used to authenticate requests to the system must appear in the list below. If they do not, use the Edit List option.

Figure 37. Transport Layer Security (TLS) Window

Note: You cannot use a configuration profile containing TLS settings to configure Intel AMT systems that have Cryptography disabled.

To configure TLS settings:

1. From the Certificate Authority drop-down list, select the certification authority.
2. From the Server Certificate Template drop-down list, select the required certificate template. If you are using a Stand-alone root CA, you can only select the default “WebServer”. If you are using an Enterprise root CA, select the template you defined for TLS (see “Certification Authorities and Templates” on page 113).
3. Define the Common Names that will be included in the Subject Name of the generated certificate (see “Defining Common Names in the Certificate Subject Name” on page 61).

4. Optionally, from the Advanced Security section, select the check boxes of the types of mutual authentication you want to enable:
   - **Use mutual authentication for remote interface**
   - **Use mutual authentication for local interface**

   Note: If you selected one of the mutual authentication options, you can also define additional TLS settings (see "Defining Advanced Mutual Authentication Settings" on page 64)

5. If you selected one of the mutual authentication options, you must define the trusted root certificates that will be used by Intel AMT systems configured with this profile (see "Defining the Trusted Root Certificates" on page 59).

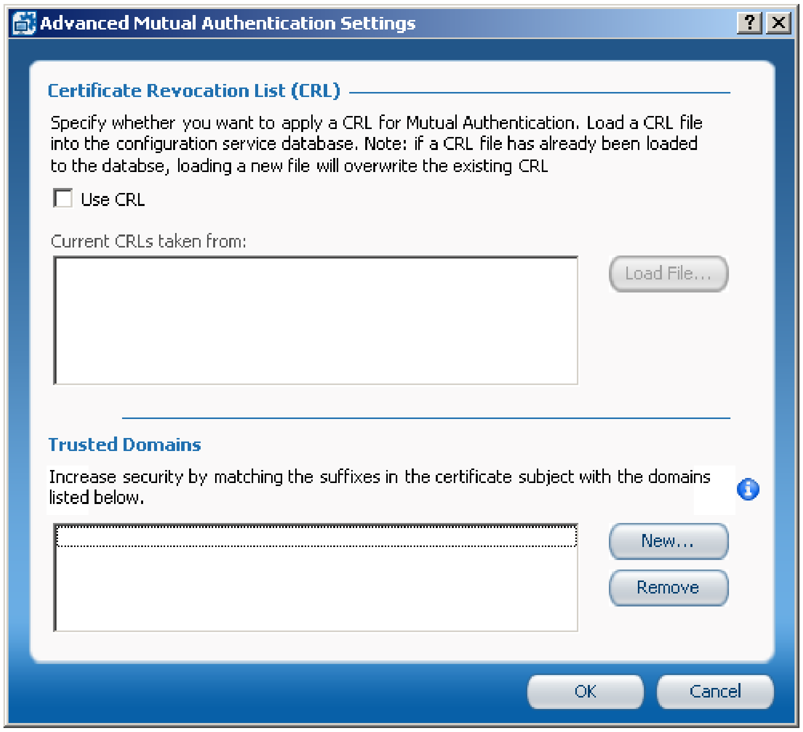
Defining Advanced Mutual Authentication Settings

The Advanced Mutual Authentication Settings window enables you to define a Certificate Revocation List (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.

You can also define the Fully Qualified Domain Name (FQDN) suffixes that will be used by mutual authentication. The Intel AMT device will validate that any client certificates used by the Intel 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 define advanced mutual TLS settings:

1. From the TLS window (Figure 37), click **Advanced**. The Advanced Mutual Authentication Settings window appears.



Advanced Mutual Authentication Settings

Certificate Revocation List (CRL)

Specify whether you want to apply a CRL for Mutual Authentication. Load a CRL file into the configuration service database. Note: if a CRL file has already been loaded to the databse, loading a new file will overwrite the existing CRL

□ Use CRL

Current CRLs taken from:

Trusted Domains

Increase security by matching the suffixes in the certificate subject with the domains listed below.

Figure 38. Advanced Mutual Authentication Settings Window

2. Optionally, define the CRL you want to use in this profile:

   a. Select **Use CRL**.

   b. Click **Load File**. The Open window appears.

   c. Browse to the location of the CRL file, select it and click **Open**. The CRL file appears in the Current CRLs taken from list.

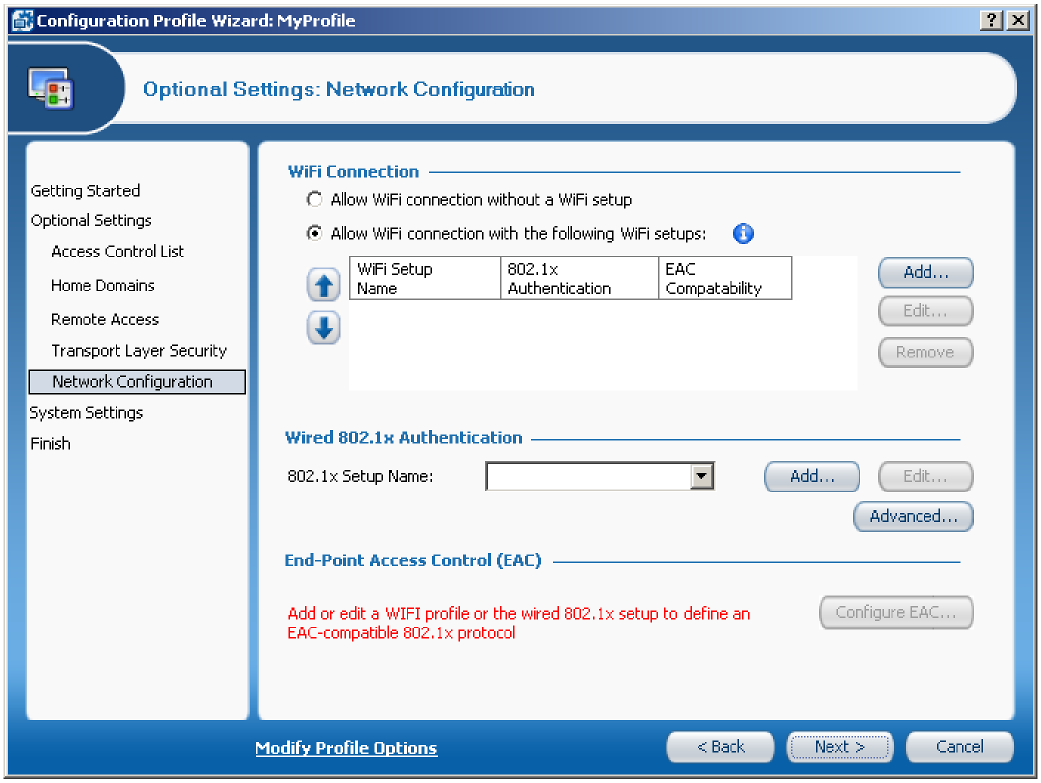
   For more information on the XML file format, see "CRL XML Format" on page 102.

3. Optionally, define the trusted domains to use in mutual authentication. To add a domain to the list, click **New** and specify the domain in the Domain Properties window. The Intel AMT system will validate that any client certificates used by the Intel SCS or Management Consoles have one of the listed suffixes in the certificate subject. If no FQDN suffixes are defined, the Intel AMT system will not validate client certificate subject names.

4. Click **OK**. The Advanced Mutual Authentication Settings window closes.

Defining Network Setups in the Profile

The Network Configuration window of the Configuration Profile Wizard enables you to define several network setups that the Intel AMT system must use. A network setup includes encryption and authentication protocol settings and can be used for wired or wireless connections.



○ Allow WiFi connection without a WiFi setup

● Allow WiFi connection with the following WiFi setups:

WiFi Setup Name	802.1x Authentication	EAC Compatability

802.1x Setup Name:

Add or edit a WIFI profile or the wired 802.1x setup to define an EAC-compatible 802.1x protocol

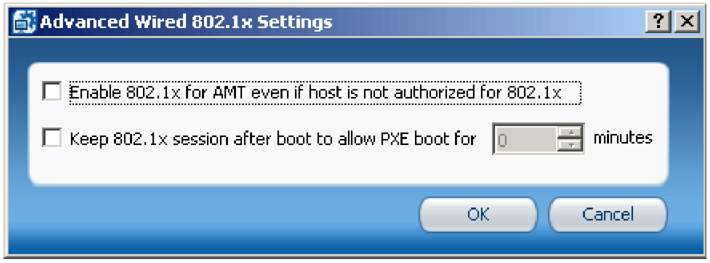
Figure 39. Network Configuration Window

To define network setups:

1. From the WiFi Connection section, select one of the following:

    - **Allow WiFi connection without a WiFi setup** — Enables WiFi connection without a WiFi setup (using the hosts WiFi settings). You can select this option only if you define a home domain in the Home Domains list and do not select a WiFi setup.
    - **Allow WiFi connection with the following WiFi setups** — If you select this option, you can perform the following to define up to 15 WiFi setups in the WiFi setup list:
        - Add a new WiFi setup to the list by clicking **Add** — See “Creating WiFi Setups” on page 67.
        - Edit an existing WiFi setup by clicking **Edit**.
        - Remove a WiFi setup from the list by clicking **Remove**.
        - Select a WiFi setup and click the Up or Down arrows to change the priority of the WiFi setup in the list.

2. If required, from the 802.1x Setup Name drop-down list select the 802.1x setup to use on a wired LAN when the Intel AMT device is active in S3, S4, or S5 power states. Optionally, you can also edit an existing 802.1x setup by clicking **Edit** or create a new 802.1x setup by clicking **Add** (see “Creating 802.1x Setups” on page 69).
3. Optionally, define advanced wired 802.1x authentication options:
   a. Click **Advanced**. The Advanced Wired 802.1x Settings window appears.



□ Enable 802.1x for AMT even if host is not authorized for 802.1x

□ Keep 802.1x session after boot to allow PXE boot for 0 minutes

Figure 40. Advanced Wired 802.1x Settings Window

   b. Select the check boxes of the options you want to enable:
      - **Enable 802.1x for AMT even if host is not authorized for 802.1x** Manageability traffic is enabled even if the host is unable to complete 802.1x authentication to the network.
      - **Keep 802.1x session open after boot to allow PXE boot for …. minutes** 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.

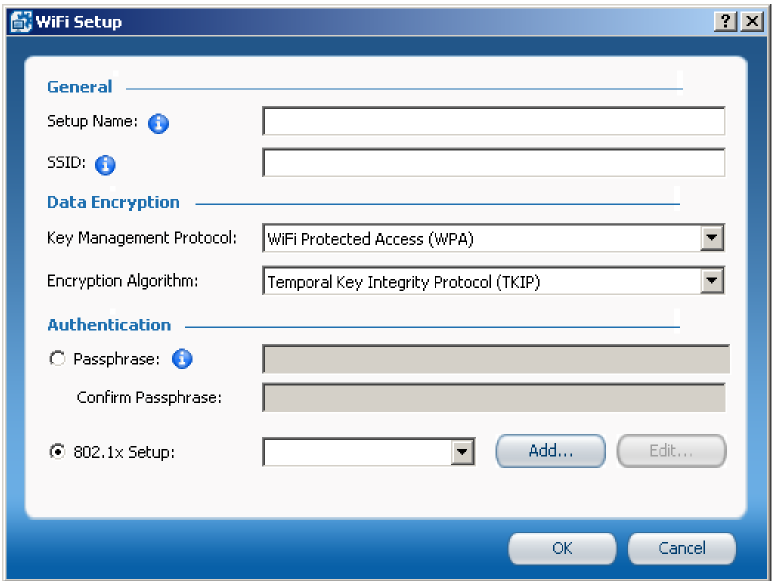
   c. Click **Ok**. The Advanced Wired 802.1x Settings window closes and the settings are saved.
4. If required, define the End-Point Access Control (EAC) parameters (see “Defining End-Point Access Control” on page 71).

Creating WiFi Setups

The WiFi setups defined in the Intel AMT device are required to enable communication with the Intel AMT device over a wireless network. These WiFi setups can also be used to enable Remote Access via a Management Presence Server (MPS) even when the computer is not in the enterprise network. In addition to the 15 WiFi setups that can be defined here, you can also enable the WiFi synchronization feature (see “Defining System Settings in the Profile” on page 72).

To create a WiFi setup:

1. From the WiFi Connection section of the Network Configuration window, click **Add**. The WiFi Setup window appears.



Setup Name:

SSID:

Key Management Protocol: WiFi Protected Access (WPA)

Encryption Algorithm: Temporal Key Integrity Protocol (TKIP)

○ Passphrase:

Confirm Passphrase:

● 802.1x Setup:

Figure 41. WiFi Setup Window

2. In the Setup Name field, enter a name for this WiFi setup. The setup name can be up to 32 characters, and must not contain (/ \\ : ; | \) characters.

3. Optionally, in the SSID field, enter a Service Set Identifier (SSID). If entered, the SSID must be a string of 1 to 32 characters naming a specific wireless LAN.

4. From the Key Management Protocol drop-down list, select one of the following:

   - **WiFi Protected Access (WPA)**
   - **Robust Security Network (RSN)**

5. From the Encryption Algorithm drop-down list, select one of the following:

   - **Temporal Key Integrity Protocol (TKIP)**
   - **Counter mode CBC MAC Protocol (CCMP)**

6. In the Authentication section, select one of the following:

   - **Passphrase** — Enter a Passphrase for the WiFi setup. The Passphrase must contain between 8 and 63 printable ASCII characters.
   - **802.1x Setup** — From the drop-down list, select the 802.1x setup to use in this WiFi setup. Optionally, you can also edit an existing 802.1x setup by clicking **Edit** or create a new 802.1x setup by clicking **Add** (see “Creating 802.1x Setups” on page 69).

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 Intel 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.

7. Click **OK**. The WiFi setup appears in the WiFi setup list.

Creating 802.1x Setups

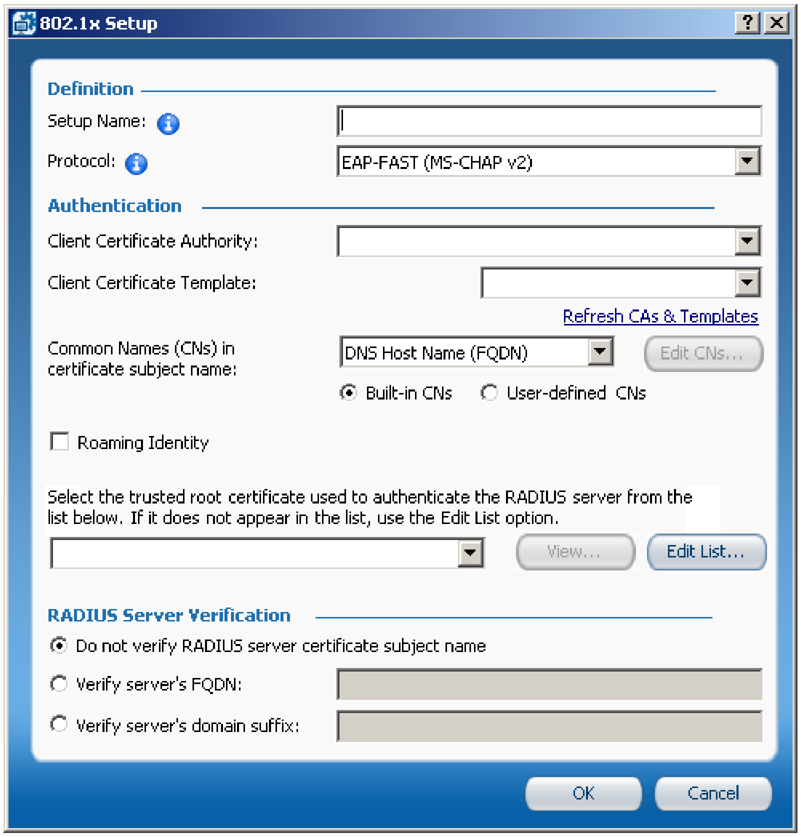
The IEEE802.1x network protocol provides an authentication mechanism to devices wishing to attach to a LAN, either establishing a point-to-point connection or preventing it if authentication fails. It is used for most wireless 802.11 access points and is based on the Extensible Authentication Protocol (EAP). You can include the 802.1x setups you define in the profile for wireless and wired connections. (The “EAP (GTC)” protocol can only be used in 802.1x wired setups.)

Note:

- You can configure 802.1x setups only for Intel AMT Releases 2.5, 2.6, 3.0, and later.
- Implementing 802.1x setups requires integration with Active Directory (see “Defining Service Settings” on page 36) and an Enterprise-root CA.

To create an 802.1x setup:

1. From the WiFi Setup window or the Wired 802.1x Authentication section of the Network Configuration window, click **Add**. The 802.1x Setup window appears.



802.1x Setup

Definition

Setup Name:

Protocol: EAP-FAST (MS-CHAP v2)

Authentication

Client Certificate Authority:

Client Certificate Template:

Refresh CAs & Templates

Common Names (CNs) in certificate subject name: DNS Host Name (FQDN) Edit CNs...

● Built-in CNs ○ User-defined CNs

□ Roaming Identity

Select the trusted root certificate used to authenticate the RADIUS server from the list below. If it does not appear in the list, use the Edit List option.

View... Edit List...

RADIUS Server Verification

● Do not verify RADIUS server certificate subject name

○ Verify server's FQDN:

○ Verify server's domain suffix:

OK Cancel

Figure 42. 802.1x Setup Window

2. In the Setup Name field, enter a name for this 802.1x setup. The setup name can be up to 32 characters, and must not contain (/ \\ : ; | \) characters.

3. From the Protocol drop-down list, select from one of the available options. The client and server authentication methods enabled in the 802.1x Setup window vary according to the protocol selected, as described in the following table.

Table 11. Protocol Options

Protocol	Trusted Root Certificate	Client Certificate Authority	Roaming Identity
EAP-TLS	Required	Required	Not available
EAP-TTLS (MS-CHAP v2)	Required	Optional	Optional
EAP-PEAP (MS-CHAP v2)	Required	Not required	Optional
EAP (GTC)	Not available	Not available	Not available
EAP-FAST (MS-CHAP v2)	Required	Required	Optional
EAP-FAST (TLS)	Required	Required	Optional
EAP-FAST (GTC)	Required	Required	Optional

4. If required, from the Client Certificate Authority drop-down list, select the Enterprise CA that the AMT system will use to request a certificate that the RADIUS server can authenticate.

Note: You can only select a Certificate Authority if it has been published in the Active Directory (unpublished CAs are not displayed in the drop-down list).

5. If required, from the Client Certificate Template drop-down list, select a template defined for creating the appropriate client certificate. The available templates will be templates where the Subject Name is supplied in the request and the usage is “Client Authentication” (see “Certification Authorities and Templates” on page 113).

6. Define the Common Names that will be included in the Subject Name of the generated certificate (see “Defining Common Names in the Certificate Subject Name” on page 61).

7. Optionally, to enable roaming, select the **Roaming Identity** check box. The user will connect to the RADIUS server with an identity of *Anonymous*.

8. If required, select the trusted root certificate that will be used in the 802.1x setup to authenticate with a RADIUS server. Optionally, you can perform the following when defining the trusted root certificate:

   - View the certificate by clicking **View**.
   - Add a new root certificate by clicking **Edit List** (see “Defining the Trusted Root Certificates” on page 59).

9. From the RADIUS Server Domain Name Verification section, select one of the following:
   - **Do not verify RADIUS server certificate subject name**
   - **Verify server’s FQDN** — Enter the FQDN of the RADIUS server
   - **Verify server’s domain suffix** — Enter the domain name suffix of the RADIUS server
10. Click **OK**. The 802.1x Setup window closes and the 802.1x setup is saved.

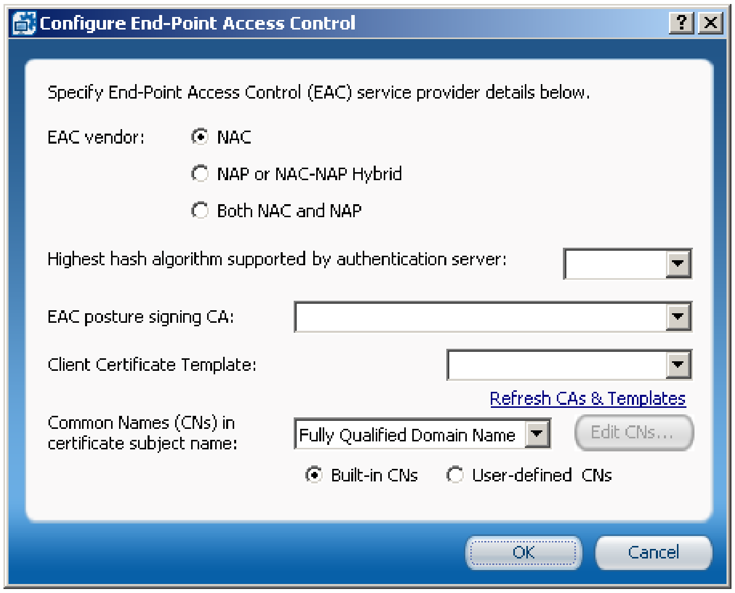
Defining End-Point Access Control

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 Intel AMT device. If the 802.1x profile’s protocol is one of the PEAP definitions, you can specify NAP or NAC-NAP hybrid authentication.

Note: Implementing EAC requires integration with Active Directory (see “Defining Service Settings” on page 36) and an Enterprise-root CA.

To define EAC:

1. From the Network Configuration window, click **Configure EAC**. The Configure End-Point Access Control window appears.



Configure End-Point Access Control

Specify End-Point Access Control (EAC) service provider details below.

EAC vendor: ● NAC
○ NAP or NAC-NAP Hybrid
○ Both NAC and NAP

Highest hash algorithm supported by authentication server:

EAC posture signing CA:

Client Certificate Template:

Common Names (CNs) in certificate subject name: Fully Qualified Domain Name

● Built-in CNs ○ User-defined CNs

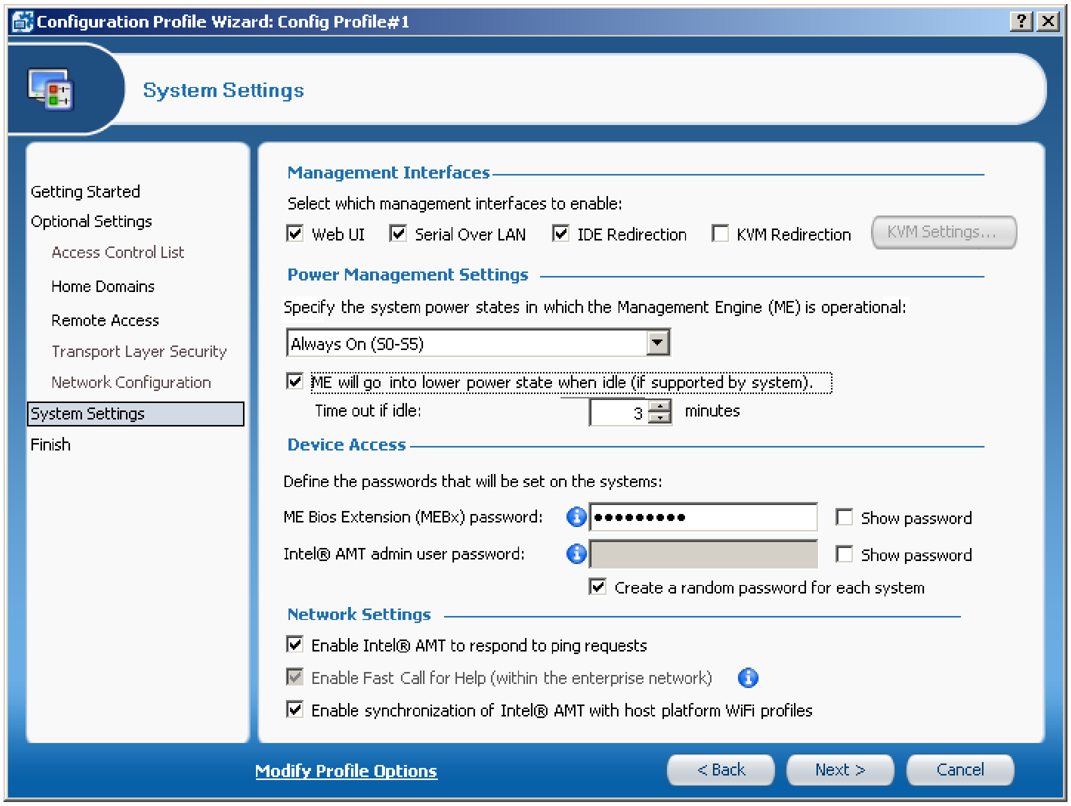
Figure 43. Configure End-Point Access Control Window

2. In the EAC vendor section, select one of the following:
   - NAC
   - NAP or NAC-NAP Hybrid
   - Both NAC and NAP

3. From the Highest hash algorithm supported by the authentication server drop-down list, select one of the following:
   - SHA-1
   - SHA-256 (supported from Intel AMT Release 6.0)
   - SHA-384 (supported from Intel AMT Release 6.0)
4. From the EAC posture signing CA drop-down list, select the certificate authority to use for issuing a client certificate for EAC posture signing.
5. From the Client Certificate Template drop-down list, select the template to use when issuing the certificate. The available templates will be templates where the Subject Name is supplied in the request (see "Certification Authorities and Templates" on page 113).
6. Define the Common Names that will be included in the Subject Name of the generated certificate (see "Defining Common Names in the Certificate Subject Name" on page 61).
7. Click **OK**. The Configure End-Point Access Control window closes.

Defining System Settings in the Profile

The System Settings window of the Configuration Profile Wizard enables you to define a profile's default network, security, and power management settings.



Management Interfaces

Select which management interfaces to enable:

☑ Web UI ☑ Serial Over LAN ☑ IDE Redirection ☐ KVM Redirection

Power Management Settings

Specify the system power states in which the Management Engine (ME) is operational:

Always On (S0-S5)

☑ ME will go into lower power state when idle (if supported by system).

Time out if idle: 3 minutes

Device Access

Define the passwords that will be set on the systems:

ME Bios Extension (MEBx) password: •••••••••• ☐ Show password

Intel® AMT admin user password: ☐ Show password

☑ Create a random password for each system

Network Settings

☑ Enable Intel® AMT to respond to ping requests

☑ Enable Fast Call for Help (within the enterprise network)

☑ Enable synchronization of Intel® AMT with host platform WiFi profiles

Figure 44. System Settings Window

To define the system settings:

1. In the Management Interfaces section, select the interfaces you want to enable with this profile:
   - **Web UI** — Enables you to manage and maintain Intel AMT systems using a browser-based interface.
   - **Serial Over LAN** — SOL enables you to remotely manage Intel AMT systems by encapsulating keystrokes and character display data in a TCP/IP stream.
   - **IDE Redirection** — IDE-R enables you to map a drive on the Intel AMT system to a remote image or drive. This functionality is generally used to reboot an Intel AMT system from an alternate drive.
   - **KVM Redirection**— See "Defining KVM Redirection Settings" on page 75.

   Note: If the OEM defined the SOL and IDE-R interfaces to be closed by default, then a Reset Configuration operation (see "Resetting Configuration of Intel AMT Systems" on page 93) will close them and they cannot be reopened without physical access to the MEBx. This is a known Firmware limitation.

2. From the drop-down list in the Power Management Settings section, select one of the following:
   - **Host is on (S0)** — The Intel AMT manageability features are available only if the operating system of the Intel AMT system is up and running.
   - **Always on (S0-S5)** — The Intel AMT manageability features are available in any of the system power states, provided the computer is connected to the power supply.
3. Optionally, if you selected *Always on (S0-S5)*, you can select the **ME will go into a lower power state when idle** check box. In the Time out if idle field, enter the minimum time (in minutes) that the ME 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.
4. In the ME BIOS Extension (MEBx) password field, enter the password used during Remote Configuration. If the MEBx password of the Intel AMT device is still the factory default, the Intel SCS will change it to the password you enter here.

5. Perform one of the following to define the password used by the Administrator ("admin") user for remote communication with the Intel AMT system:

   - To automatically create a different password for each Intel AMT system configured with this profile, ensure that the **Create a random password for each system** check box is selected.
   - To set the same password for all Intel AMT systems configured with this profile, clear the **Create a random password for each system** check box and enter a password. The password must be at least 8 characters, with at least one of each of the following:
     - A number
     - A non alpha-numeric character (note that "_" is considered alpha-numeric)
     - A lower case latin letter
     - An upper case latin letter

6. Optionally, select **Enable Intel® AMT to respond to ping requests**. When this check box is selected, the Intel AMT device will respond to a ping if the host platform does not.

7. Optionally, select **Enable Fast Call for Help (within the enterprise network)**. When this check box is selected, if the computer is inside the enterprise network the user can initiate a connection request to connect to a management console. (To enable the Fast Call for Help feature from outside the enterprise network, see "Defining Remote Access in the Profile" on page 56.)

8. Intel AMT Release 6.0 includes support for synchronization of the WiFi profiles present on the host platform with the WiFi setups defined in the Intel AMT device. When the **Enable Synchronization of Intel® AMT with host platform WiFi profiles** check box is selected this support is enabled.
   The synchronization is performed by a third party application, such as the Intel PROSet/Wireless Software, in the following way:

   - **User-defined profiles** — When a user performs a successful connection to a wireless network with a WiFi profile that is not defined in the Intel AMT, the third party application displays a pop-up message asking the user if he wants to add the profile to the Intel AMT (making the profile available for use by the Intel AMT). Up to eight user defined profiles can be stored in the Intel AMT (in addition to the WiFi setups defined in "Creating WiFi Setups" on page 67).
   - **IT-defined profiles** — Wi-Fi profiles that are added to the host operating system through a Group Policy by IT administrators will be added to the Intel AMT. Up to 16 IT-defined profiles can be stored in the Intel AMT Release 6.0 (15 for previous Intel AMT Releases).

Note:

- User-defined profiles can only be "synchronized" by the user. They can not be altered or added from a remote computer.
- WiFi profiles are only added to the Intel AMT if the Wi-Fi protocol is supported by the Intel AMT.

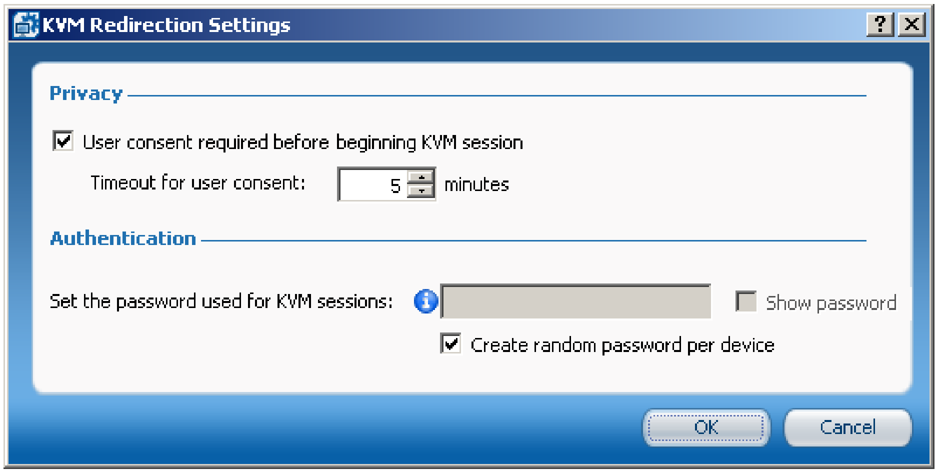
Defining KVM Redirection Settings

Intel AMT Release 6.0 introduces support for the Keyboard, Video and Mouse (KVM) capability. KVM enables remote control of an Intel AMT system using a remote keyboard and mouse and viewing the managed system's screen output at a remote monitor. KVM is based on the RealVNC Limited* Remote Frame Buffer (RFB) protocol.

The following procedure describes how to set the KVM settings in the configuration profile that determine how the Intel AMT system handles KVM connection requests.

To define KVM settings:

1. From the System Settings window, click **KVM Settings**. The KVM Redirection Settings window appears.



KVM Redirection Settings

Privacy

☑ User consent required before beginning KVM session

Timeout for user consent: 5 minutes

Authentication

Set the password used for KVM sessions: □ Show password

☑ Create random password per device

Figure 45. KVM Redirection Settings Window

2. If you want to define that the user of the Intel AMT system must consent to KVM connections, select **User consent required before beginning KVM session**. If this check box is selected, a pop-up window appears on the Intel AMT system when a KVM connection request is processed. The window contains a code number that the user must provide (by telephone) to the person trying to connect to his computer. The **Timeout for user consent** field determines the maximum time (in minutes) allocated for the user consent process. If the user consent process is not completed in this time, a new KVM connection request must be sent.
3. In the Authentication section, define the password to use for KVM sessions. By default, a random password is created for each Intel AMT system. If you want to create one password for all Intel AMT systems configured with this profile, clear the **Create random password per device** check box and enter the password.
4. Click **OK**. The KVM Redirection Settings window closes.

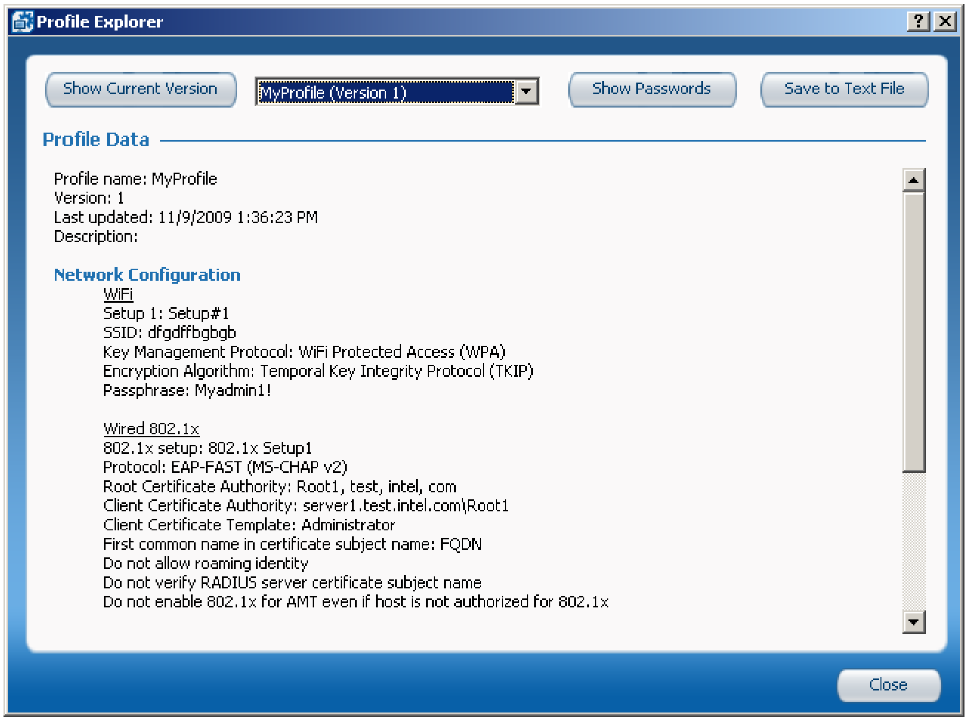
Viewing Profile History

The Intel SCS enables you to keep track of changes that were made to configuration profiles. If Intel AMT systems have been configured with a profile, when you make changes to the profile a new version of the profile is automatically created.

To view profile history:

1. Perform one of the following:
   - Right-click the required profile and select **View Profile Versions**
   - Select the profile and then select **Actions** > **View Profile Versions**

   The Profile Explorer window appears.



Profile name: MyProfile
Version: 1
Last updated: 11/9/2009 1:36:23 PM
Description:

Network Configuration
WiFi
Setup 1: Setup#1
SSID: dfgdffbgbgb
Key Management Protocol: WiFi Protected Access (WPA)
Encryption Algorithm: Temporal Key Integrity Protocol (TKIP)
Passphrase: Myadmin1!

Wired 802.1x
802.1x setup: 802.1x Setup1
Protocol: EAP-FAST (MS-CHAP v2)
Root Certificate Authority: Root1, test, intel, com
Client Certificate Authority: server1.test.intel.com\Root1
Client Certificate Template: Administrator
First common name in certificate subject name: FQDN
Do not allow roaming identity
Do not verify RADIUS server certificate subject name
Do not enable 802.1x for AMT even if host is not authorized for 802.1x

Figure 46. Profile Explorer Window

2. The settings of the configuration profile are displayed in the Profile Data section. You can perform the following from the Profile Explorer window:
   - View the settings of a specific version of the profile by selecting the version from the drop-down list.
   - View the settings of the current version of the profile by clicking **Show Current Version**.
   - Save the settings of the profile version to an RTF text file by clicking **Save to Text File**.
3. Click **Close**. The Profile Explorer window closes.

6

Configuring with TLS-PSK

This chapter describes how to prepare the Intel SCS and the Intel AMT systems for setup and configuration using the TLS-PSK (Pre-Shared Key) protocol.

It includes the following topics:

- About Configuring with TLS-PSK
- Importing Configuration Keys from a File
- Creating and Exporting Configuration Keys to a USB Drive
- Creating and Printing Configuration Keys

About Configuring with TLS-PSK

The TLS-PSK protocol uses a TLS-PSK configuration key to establish secure communication during the configuration process.

Note: You must use the TLS-PSK protocol in the following Intel AMT versions: 2.0/2.1/2.5.
For Intel AMT versions 2.2/2.6 or 3.0 and later, you can use the TLS-PSK protocol or the PKI infrastructure (see "Remote Configuration" on page 104).

The configuration key must be installed on both the Intel AMT system and in the database, and contains the following:

- **Provisioning ID (PID)** — An 8 character identifier
- **Provisioning Passphrase (PPS)** — A 32 character key
- **Current MEBx Password** — The administrator password defined in the Intel AMT device's MEBx by the OEM
- **New MEBx Password** — The password with which the Intel SCS will replace the current administrator password during configuration

Importing Configuration Keys from a File

If the OEM has pre-configured Intel AMT systems with configuration keys, you must import them into the database from the file that he supplies. No further action is required.

To import keys from a file:

1. Copy the *setup.bin* file containing the keys to a folder that the computer running the Service can access.
2. Select **Tools** > **TLS-PSK Configuration Keys > Import Keys from File**. The Open window appears
3. Navigate to the folder where the *setup.bin* file is located, select the file and click **Open**. The keys are imported and a message appears with details of how many keys were successfully imported.

Creating and Exporting Configuration Keys to a USB Drive

The Export Keys wizard enables you to create and export configuration keys to a *Setup.bin* file on a USB drive. You can then use the USB drive to install the keys on the Intel AMT system in the following ways:

- Insert the USB drive into a USB port of the Intel AMT system, and restart the system.
- When using the Activator utility, you can select the *Setup.bin* file containing the keys.

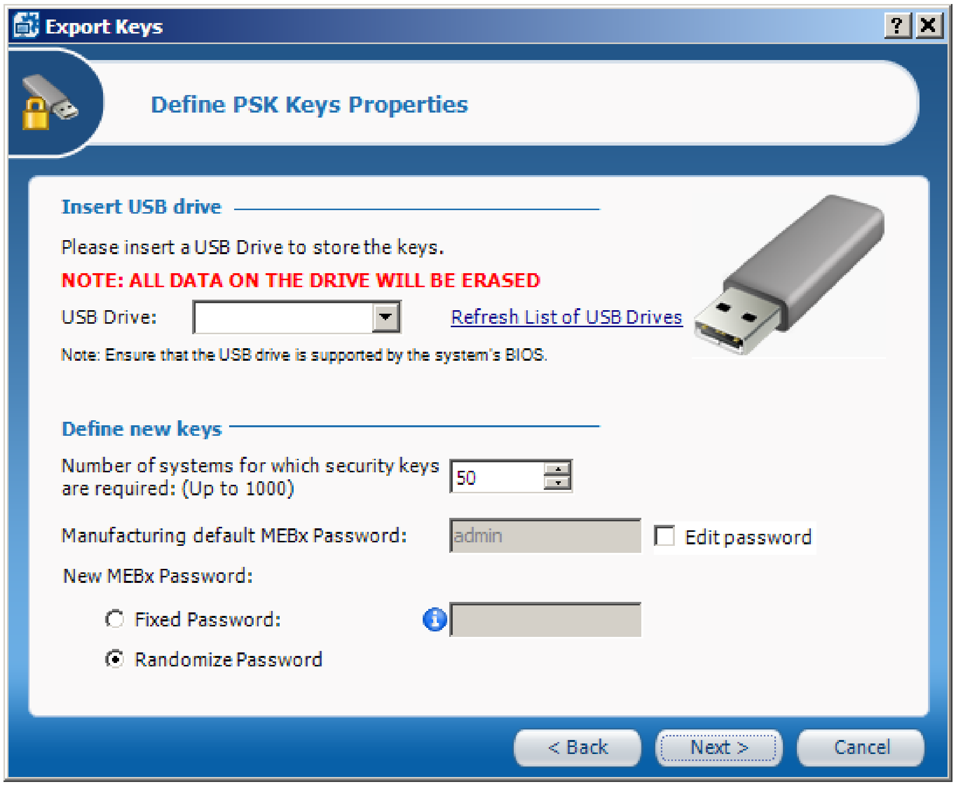
For more information, see the *Intel® vPro™ Technology Activator Utility Release Notes and User Guide*.

Note:

- Because of the sensitivity of the PID/PPS pairs, once you export keys to a USB drive, ensure that the drive does not fall into unauthorized hands.
- The Intel SCS does not restrict the size of USB drive you can use. However, the computer's BIOS must provide full support for the selected USB drive and be able to perform reboot from it.

To create and export keys to a USB drive:

1. Attach a USB drive to the computer running the Service. The USB drive will be reformatted as a bootable device by the following steps.
2. Select **Tools** > **TLS-PSK Configuration Keys > Export Keys to USB Drive**. The Welcome window of the Export Keys wizard appears.
3. Click **Next**. The Define PSK Keys Properties window appears.



Export Keys

Define PSK Keys Properties

Insert USB drive

Please insert a USB Drive to store the keys.

NOTE: ALL DATA ON THE DRIVE WILL BE ERASED

USB Drive: Refresh List of USB Drives

Note: Ensure that the USB drive is supported by the system's BIOS.

Define new keys

Number of systems for which security keys are required: (Up to 1000) 50

Manufacturing default MEBx Password: admin □ Edit password

New MEBx Password:

○ Fixed Password:

● Randomize Password

Figure 47. Define PSK Keys Properties Window

4. From the USB Drive drop-down list, select the USB drive.

5. In the number of systems for which security keys are required field, enter the number of keys that you want to create (up to 1000 keys).

6. Optionally, click **Edit password** to change the MEBx password that was entered in the firmware by the manufacturer.

7. In the New MEBx Password section, select one of the following:

   - **Fixed Password** — Select to use the same password with all the keys, and enter the password that you want to use.

   - **Randomize Password** — Select to create a different, random password for each key.

8. Click **Next**.

9. Confirm that you want to format the drive and complete the process. The wizard displays a progress bar.

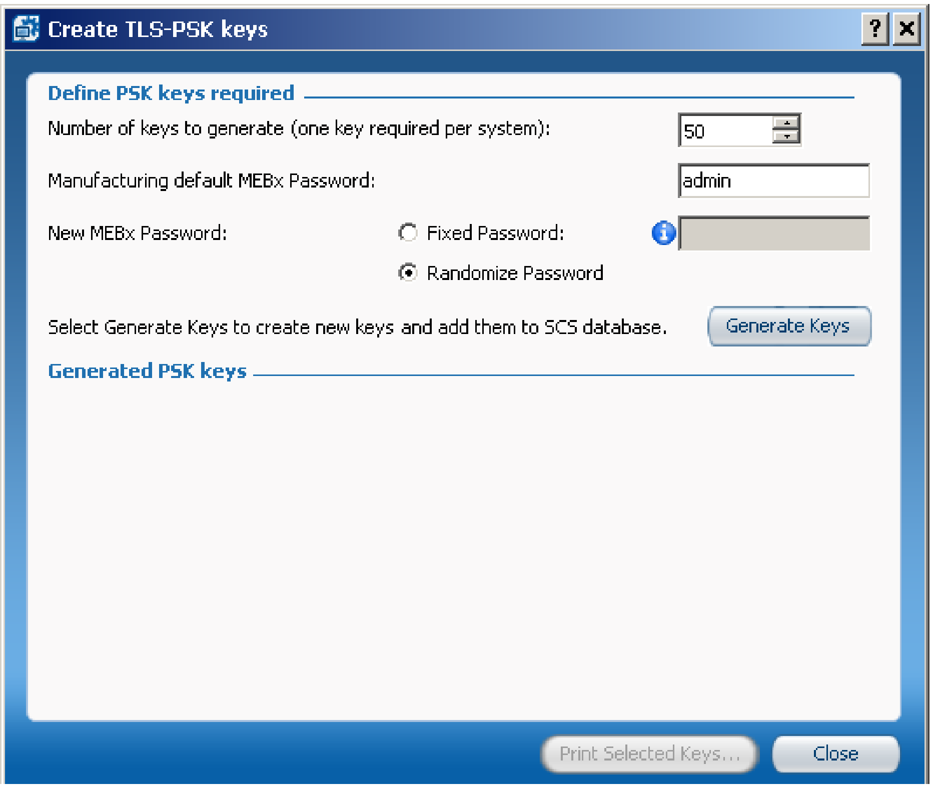
10. When the wizard indicates the process is complete, click **Finish** to exit the wizard.

Creating and Printing Configuration Keys

Instead of using a USB drive to install configuration keys on the Intel AMT systems (see “Creating and Exporting Configuration Keys to a USB Drive” on page 78), you can create and print keys and then manually insert them into the MEBx of the Intel AMT systems

To create and print configuration keys:

1. Select **Tools** > **TLS-PSK Configuration Keys** > **Add Security Keys**.
   The Create TLS-PSK Keys window appears.



Create TLS-PSK keys

Define PSK keys required

Number of keys to generate (one key required per system): 50

Manufacturing default MEBx Password: admin

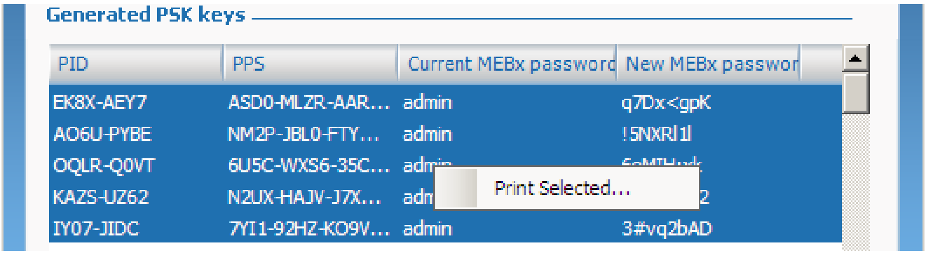
New MEBx Password: ○ Fixed Password: ● Randomize Password

Select Generate Keys to create new keys and add them to SCS database.

Generated PSK keys

Figure 48. Create TLS-PSK Keys Window

2. In the Number of keys to generate field, enter the number of keys that you want to create.
3. In the Manufacturing default MEBx Password field, enter the MEBx password that was entered in the firmware by the manufacturer.
4. In the New MEBx Password section, select one of the following:
   - **Fixed Password** — Select to use the same password with all the keys, and enter the password that you want to use.
   - **Randomize Password** — Select to create a different, random password for each key.
5. Click **Generate Keys**. The generated key values are added to the database and appear in the Generated PSK keys section.



Generated PSK keys

PID	PPS	Current MEBx password	New MEBx password
EK8X-AEY7	ASD0-MLZR-AAR...	admin	q7Dx<gpK
AO6U-PYBE	NM2P-JBL0-FTY...	admin	!5NXRl1l
OQLR-Q0VT	6U5C-WXS6-35C...	admin	6oMTHuxk
KAZS-UZ62	N2UX-HAJV-J7X...	adm	2
IY07-JIDC	7YI1-92HZ-KO9V...	admin	3#vq2bAD

Figure 49. List of Generated Keys

6. To print the list:

   a. Hold down the <Ctrl> key and select the keys that you want to print.

   b. Click **Print Selected Keys** (or right-click the selection and select **Print Selected**). The Print confirmation message appears.

   c. Click **Yes** and select the printer. You can now insert these configuration keys into the MEBx of the Intel AMT systems.

7. Click **Close**. The Create TLS-PSK Keys window closes.

7

Viewing and Editing Intel AMT Systems

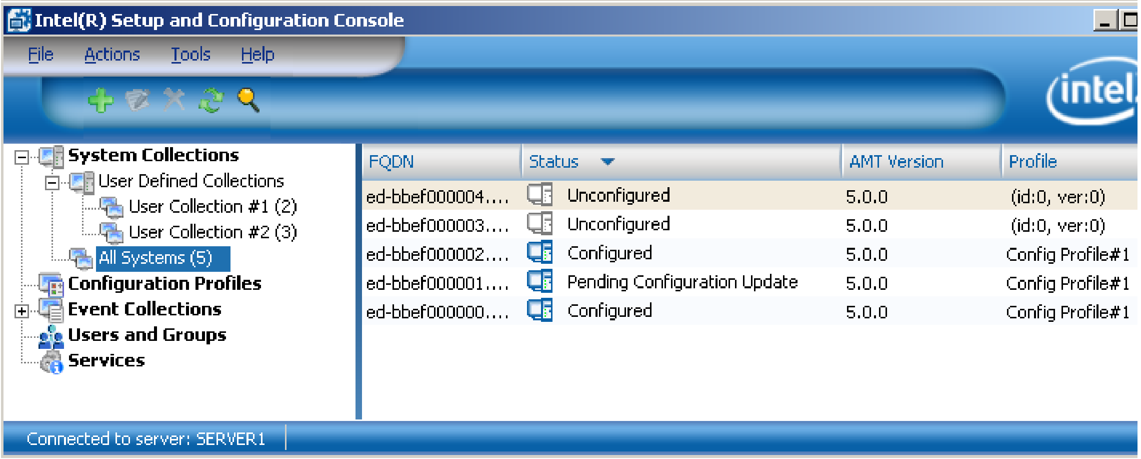
This chapter describes how to view and modify the settings of Intel AMT systems.

It includes the following topics:

- About Intel AMT Systems and System Collections
- Intel AMT System Configuration States
- Creating a System Collection
- Searching for Intel AMT Systems
- Viewing and Changing Settings of an Intel AMT System
- Performing Operations on a Collection

About Intel AMT Systems and System Collections

The Intel AMT systems and system collections are displayed in the *System Collections* node of the Console tree. (The Console displays a maximum of 1000 systems per collection.)



FQDN	Status	AMT Version	Profile
ed-bbef000004....	Unconfigured	5.0.0	(id:0, ver:0)
ed-bbef000003....	Unconfigured	5.0.0	(id:0, ver:0)
ed-bbef000002....	Configured	5.0.0	Config Profile#1
ed-bbef000001....	Pending Configuration Update	5.0.0	Config Profile#1
ed-bbef000000....	Configured	5.0.0	Config Profile#1

Connected to server: SERVER1

Figure 50. System Collections Node

When you click a collection in the left pane, the systems in that collection appear in the right pane.

The following table describes the actions you can perform from the *System Collections* node. (You cannot edit or delete the default *All Systems* collection.)

Table 12. System Collections Node Actions

Action	How to...
Create a system collection	See “Creating a System Collection” on page 85
Edit a system collection	Right-click the collection and select **Edit System Collection**
Delete a system collection	Right-click the collection and select **Delete System Collection** (Deleting a collection does not delete the systems in the collection.)
Search for a system	See “Searching for Intel AMT Systems” on page 87
View and edit system settings	See “Viewing and Changing Settings of an Intel AMT System” on page 89
Delete a system	• Right-click the system and select **Delete System** • Select the system, and then from the toolbar click ✕ or select **Actions** > **Delete System**
Refresh the displayed list of systems in a collection	• Right-click the collection and select **Refresh Systems** • From the toolbar, click ⟳
Check if the Intel SCS can connect to the system	Right-click the system and select **Test Connectivity** (This action checks if the Intel SCS can perform Intel AMT tasks and is not just a ping response check.)
Perform operations on a collection and view operations history	See “Performing Operations on a Collection” on page 94
Manually add details of an Intel AMT system to the database	Right-click **All Systems** and select **Add System Definition** (Use this option only if you want to send configuration requests to the Intel SCS using “Hello” messages as described in “Send a Configuration Request to the Intel SCS” on page 41.)

Note: You can also perform the actions on single systems from the Search Results list of the Search Systems window (see “Searching for Intel AMT Systems” on page 87).

Intel AMT System Configuration States

Each Intel AMT system stored in the database can be in one of the following states:

- **Configured** — The system is configured.
- **Configuration Failed** — The Intel SCS failed to configure the system.
- **Configuration Update Failed** — The Intel SCS failed to perform a configuration update on the system.
- **Unconfiguration Failed** — The Intel SCS failed to unconfigure the system and the system's configuration status is not known.
- **Missing Configuration Data** — A configuration request was received but it is missing some data, such as a profile.
- **Pending Configuration** — A configuration request exists but has not yet been performed on the system.
- **Pending Configuration Update** — A configuration update request exists but has not yet been performed on the system.
- **Pending Unconfiguration** — An unconfiguration request exists but has not yet been performed on the system.
- **Unconfigured** — The system is unconfigured.
- **Pending Hello Message** — An entry for the system has been added to the database. The system will be configured when the Service receives a "Hello" message sent by the system or the Activator. Repeated Hello messages sent from the same IP address within ~10 seconds are ignored.
- **FQDN in use by other system** — An Intel AMT system with a different UUID has been configured with this FQDN.
- **Unknown** — The Intel SCS does not know the status of the system.

Note: When the combined number of systems in the *Missing Configuration Data* and *Pending Hello Message* states reaches the limit (100000), further Hello messages and configuration requests with missing data are ignored.

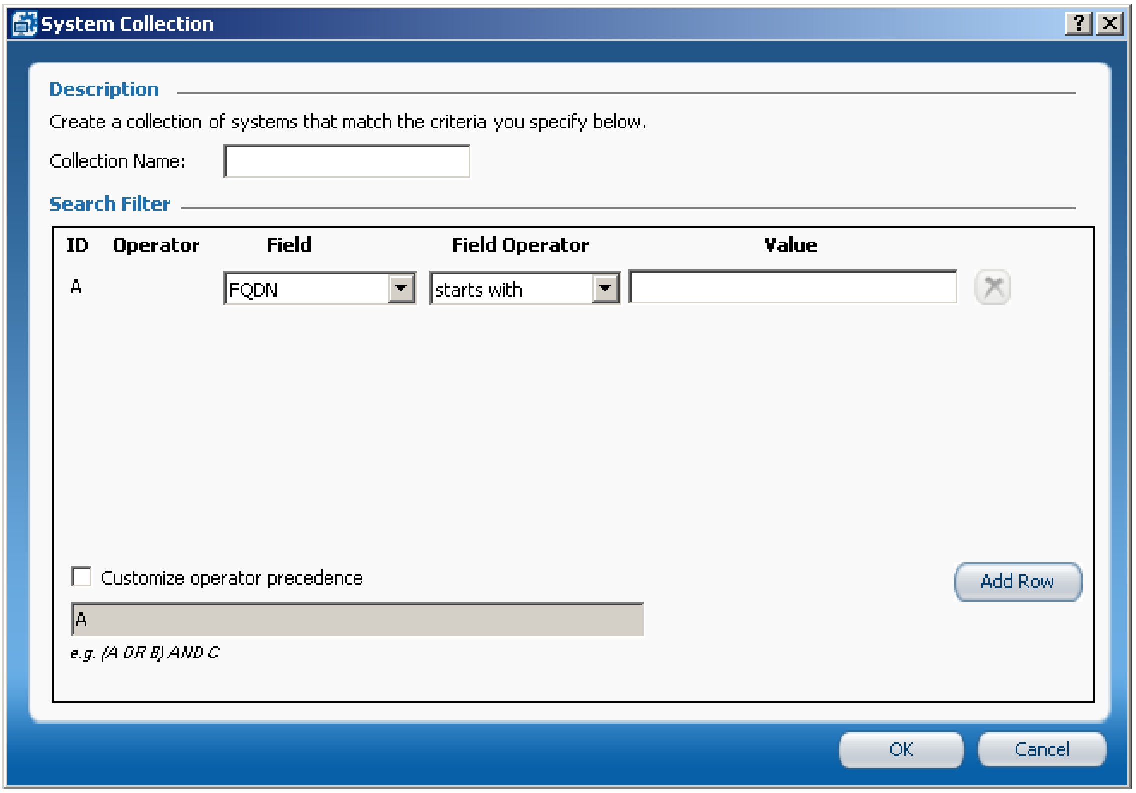
Creating a System Collection

The Console enables you to create multiple logical groups of Intel AMT systems, called system collections, based on filter conditions that you define.

To create a system collection:

1. From the Console tree, select **System Collections** and perform one of the following:
   - Right-click and select **Create System Collection**
   - From the toolbar, click or select **Actions** > **Create System Collection**

   The System Collection window appears.



Create a collection of systems that match the criteria you specify below.

Collection Name:

ID	Operator	Field	Field Operator	Value
A		FQDN	starts with	

□ Customize operator precedence

A

e.g. (A OR B) AND C

Figure 51. System Collection Window

2. In the Collection Name field, enter a descriptive name for this collection.
3. Define the filter conditions as described in “Defining a System Filter” on page 86.
4. Click **OK**. The System Collections window closes and the collection appears in the *System Collections* > *User Defined Collections* node of the Console tree.

Defining a System Filter

When creating a collection or searching for systems (see “Searching for Intel AMT Systems” on page 87), the Console enables you to create conditions to filter the systems. You can also customize the operator precedence of the filter condition rows by selecting the **Customize operator preference** check box and adding brackets to the condition ID codes (A, B etc.).

You can delete a condition by clicking the ✖ icon next to the condition.

To define a system filter:

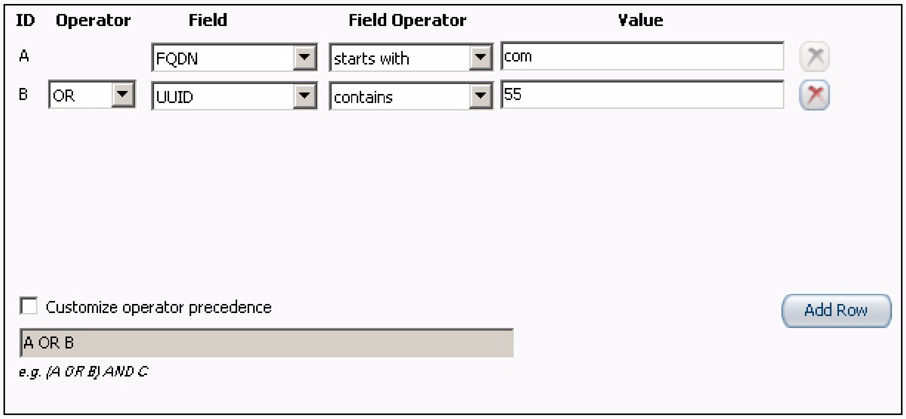
1. Define the filter condition in row A as described in the following table.

Table 13. System Filter Options

Field	Field Operator	Value
FQDN	• starts with • ends with • contains • equals	A string containing the required part of the host name that you want to include in the filter.
UUID		A string containing the required part of the system’s UUID that you want to include in the filter.
Last Configuration Time	• >= • <	By default, the current date and time is displayed in the Value field of these options. You can edit the value directly in the field or click the drop-down list arrow to select a date from a calendar.
Last Connection Time		
Status	in	From the drop-down list, select one or more configuration states (see “Intel AMT System Configuration States” on page 84). Hold down the <Ctrl> or <Shift> keys during selection.
Profile	in	From the drop-down list, select one or more profiles (hold down the <Ctrl> or <Shift> keys during selection).

2. Optionally, define more filter conditions:

   a. Click **Add Row**. A new filter condition row appears under the existing rows.



ID	Operator	Field	Field Operator	Value
A		FQDN	starts with	com
B	OR	UUID	contains	55

□ Customize operator precedence

A OR B

e.g. (A OR B) AND C

Figure 52. System Filter Example

   b. From the first drop-down list, select one of the following operators to define the relationship of this filter condition with the other filter conditions:

      - **AND** — Include the system only if this condition and the previous condition are both true
      - **OR** — Include the system if either this condition or the previous condition are true

   c. Define the remaining filter conditions as described in Table 13.

   d. Optionally, repeat steps a through c to add additional filter conditions.

3. If required, select the **Customize operator precedence** check box and define an alternative order for the filter conditions.

Searching for Intel AMT Systems

The Console enables you to search for Intel AMT systems in the database and then perform actions on them directly from the search results.

To search for systems:

1. From the Console tree, select **System Collections** and perform one of the following:

   - Right-click and select **Search for Systems**
   - From the toolbar, click 🔍 or select **Actions** > **Search for Systems**

The Search for Systems window appears.

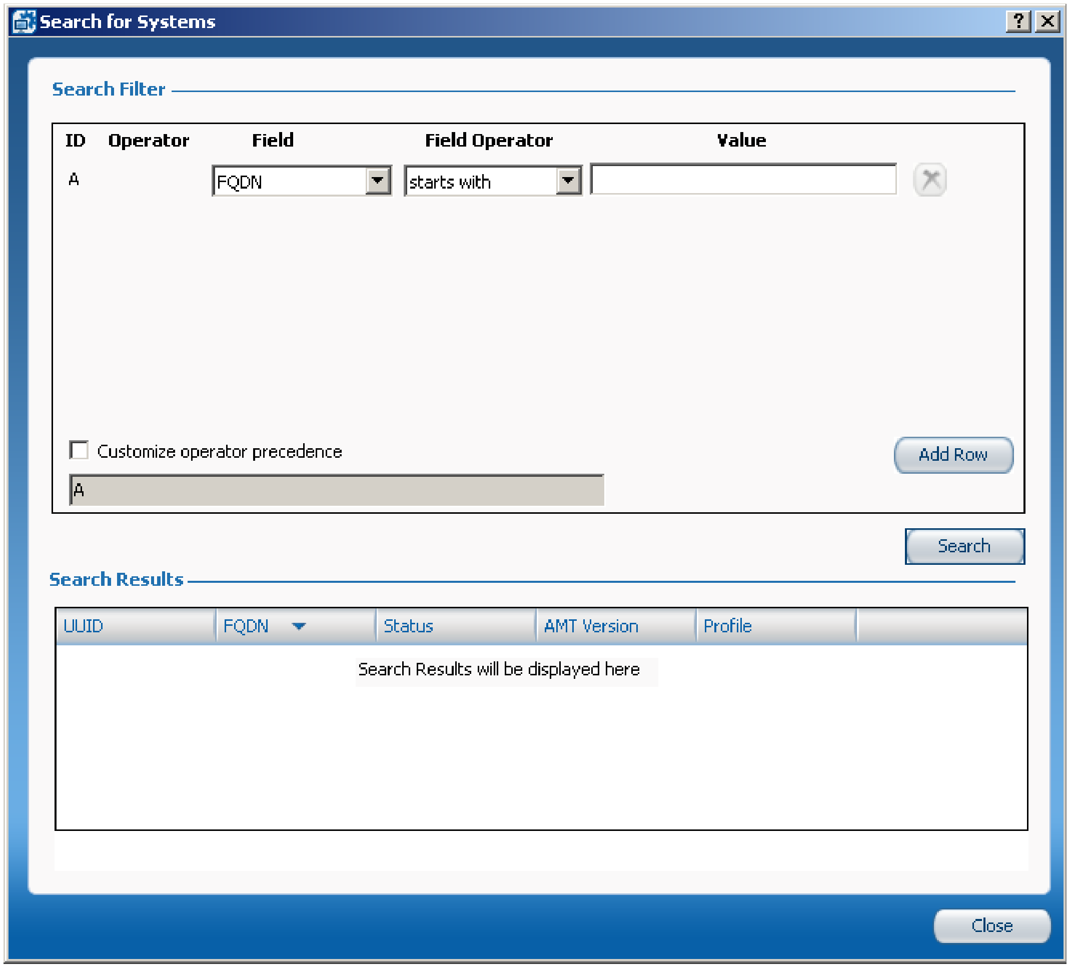


Figure 53. Search for Systems Window

2. Define the filter conditions as described in “Defining a System Filter” on page 86.
3. Click **Search**. The systems that meet the filter conditions appear in the Search Results list. If the system you are searching for is not in the Search Results list, modify the filter conditions and click **Search**.
4. Optionally, select one or more of the systems in the Search Results list (hold down the <Ctrl> or <Shift> keys during selection), right-click and select the required action.
5. Click **Close**. The Search for Systems window closes.

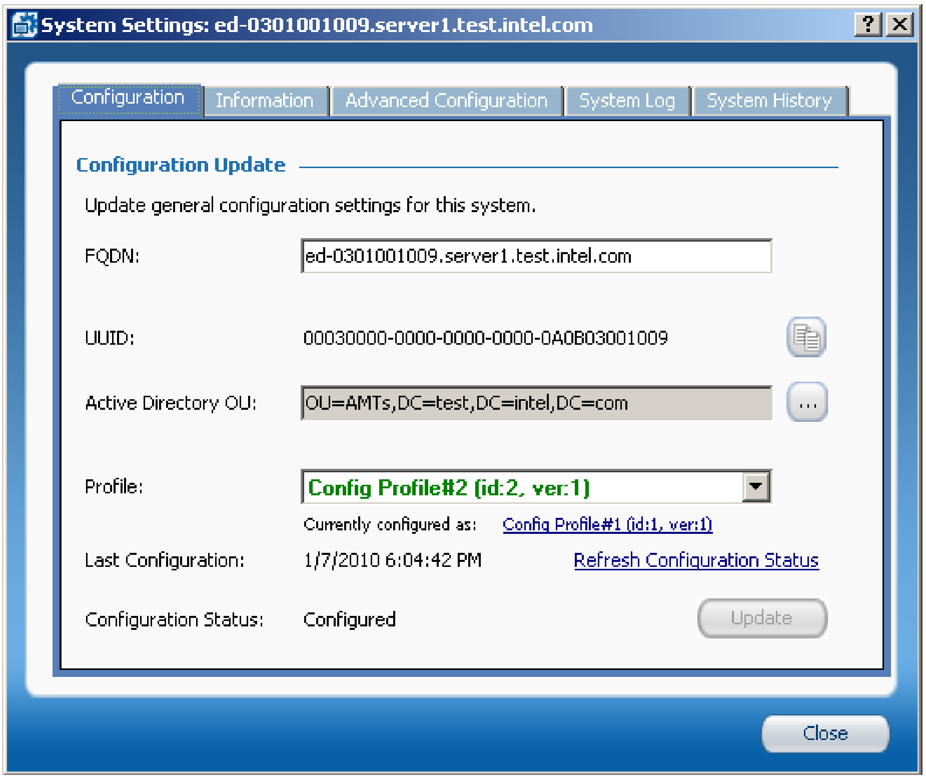
Viewing and Changing Settings of an Intel AMT System

You can view and change the settings of an Intel AMT system configuration from any of the lists of systems in the Console.

To view or change a systems settings:

1. Perform one of the following:
    - Right-click the required system and select **Edit System**
    - Select the system, and then from the toolbar click or select **Actions** > **Edit System**

    The Configuration tab of the System Settings window appears.



Configuration Update

Update general configuration settings for this system.

FQDN: ed-0301001009.server1.test.intel.com

UUID: 00030000-0000-0000-0000-0A0B03001009

Active Directory OU: OU=AMTs,DC=test,DC=intel,DC=com

Profile: Config Profile#2 (id:2, ver:1)

Currently configured as: Config Profile#1 (id:1, ver:1)

Last Configuration: 1/7/2010 6:04:42 PM Refresh Configuration Status

Configuration Status: Configured

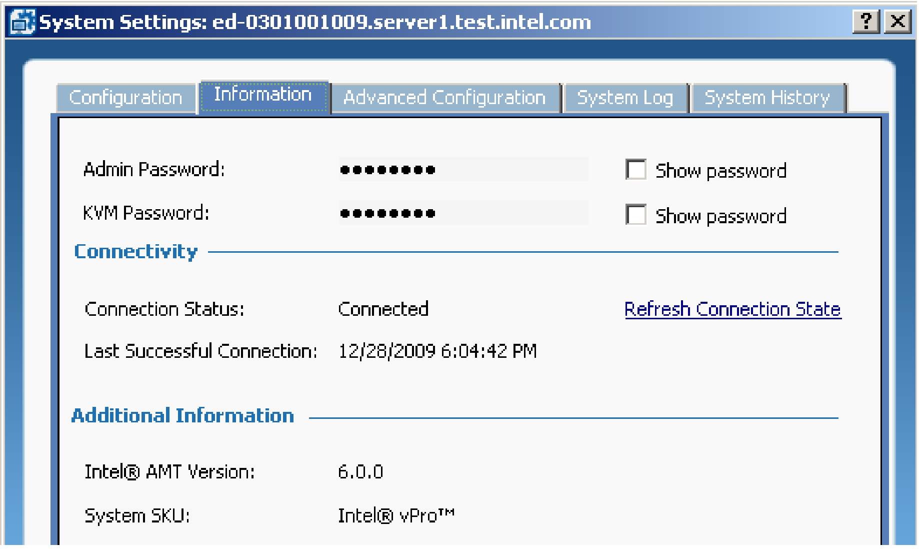
Figure 54. System Settings - Configuration Tab

2. The fields that you can change in the Configuration tab depend on the status of the system. Optionally, edit the required fields as described in the following table.

Table 14. System Configuration Options

Field/Option	Description
FQDN	The Fully Qualified Domain Name of the system.
UUID	The Universally Unique Identifier of the system.
Active Directory OU	The Organizational Unit where the system is stored in Active Directory. This field is displayed only if the Intel SCS is defined to work in integrated mode with Active Directory (see “Defining Service Settings” on page 36).
Profile	A drop-down list is displayed, enabling you to select the profile that you want to use to configure the system. If the Intel AMT system is currently configured with a different profile (or version) from the one selected in the drop-down list, a link to the current profile information is displayed. Double-click the link to open the Profile Explorer window and view the profile settings (for more information, see “Viewing Profile History” on page 76). You can also change the profiles of all systems in a collection (see “Performing Operations on a Collection” on page 94).
Last Configuration	The date and time that the last configuration was performed.
Configuration Status	The current configuration status of the system. (See “Intel AMT System Configuration States” on page 84.)
Update	Ensure that the values of the fields are correct and then click **Update** to send an updated configuration request. The FQDN, ADOU, and Profile information is sent to the Service for processing.

3. If the system is configured, click the **Information** tab. The Information tab appears displaying the system’s network administrator password and the connectivity status and history of the system.



System Settings: ed-0301001009.server1.test.intel.com

Admin Password: •••••••• □ Show password

KVM Password: •••••••• □ Show password

Connectivity

Connection Status: Connected — Refresh Connection State

Last Successful Connection: 12/28/2009 6:04:42 PM

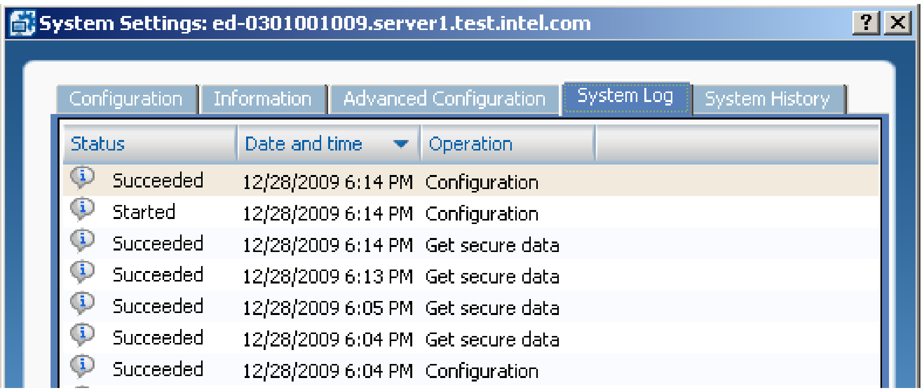
Additional Information

Intel® AMT Version: 6.0.0

System SKU: Intel® vPro™

Figure 55. System Settings - Information Tab

4. If the system is configured, click the **Advanced Configuration** tab. The Advanced Configuration tab appears. Optionally, select the operations you want to perform on this Intel AMT system:
   - **Maintenance** — See "Manually Run Maintenance Operations" on page 92.
   - **Configuration Reset** — See "Resetting Configuration of Intel AMT Systems" on page 93.
5. Click the **System Log** tab. The System Log tab appears displaying all events that have occurred in the last seven days that involve this system.



System Settings: ed-0301001009.server1.test.intel.com

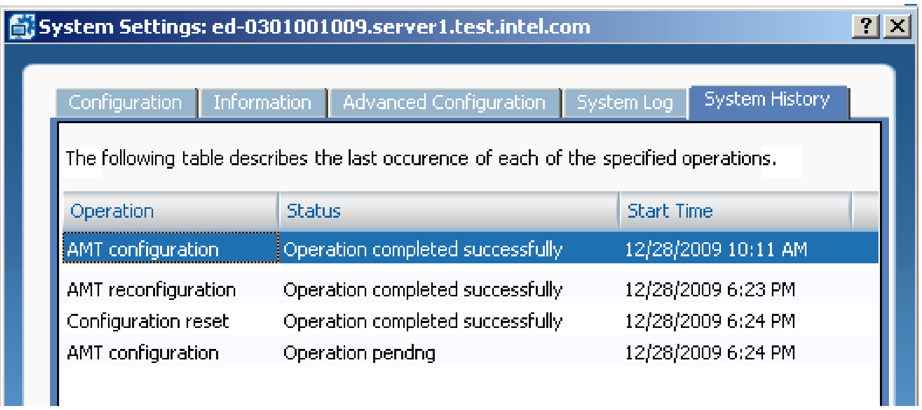
Status	Date and time	Operation
Succeeded	12/28/2009 6:14 PM	Configuration
Started	12/28/2009 6:14 PM	Configuration
Succeeded	12/28/2009 6:14 PM	Get secure data
Succeeded	12/28/2009 6:13 PM	Get secure data
Succeeded	12/28/2009 6:05 PM	Get secure data
Succeeded	12/28/2009 6:04 PM	Get secure data
Succeeded	12/28/2009 6:04 PM	Configuration

Figure 56. System Settings - System Log Tab

Note:

- You can view the details of an event by double-clicking the event.
- For more information about logs and events, see "Viewing the Intel SCS Events" on page 96.

6. Click the **System History** tab. The System History tab appears displaying the last occurrence of each type of operation.



The following table describes the last occurence of each of the specified operations.

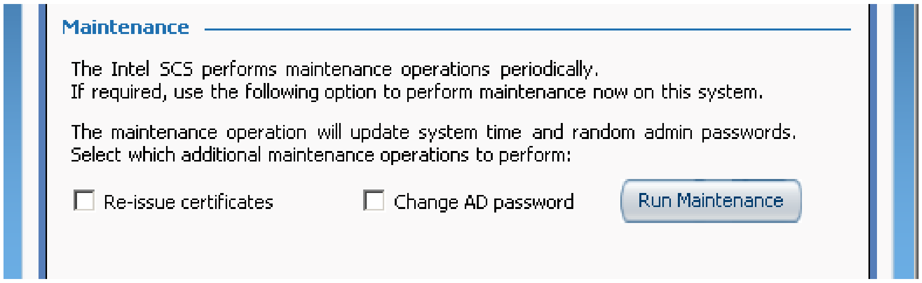
Operation	Status	Start Time
AMT configuration	Operation completed successfully	12/28/2009 10:11 AM
AMT reconfiguration	Operation completed successfully	12/28/2009 6:23 PM
Configuration reset	Operation completed successfully	12/28/2009 6:24 PM
AMT configuration	Operation pendng	12/28/2009 6:24 PM

Figure 57. System Settings - System History Tab

7. Click **Close**. The System Settings window closes and the status of the system is updated according to the settings you selected.

Manually Run Maintenance Operations

The Intel SCS performs several maintenance tasks automatically (see "Automatic Maintenance" on page 5). The Maintenance options enable you to manually run the automatic maintenance tasks.



The Intel SCS performs maintenance operations periodically.
If required, use the following option to perform maintenance now on this system.

The maintenance operation will update system time and random admin passwords.
Select which additional maintenance operations to perform:

☐ Re-issue certificates ☐ Change AD password Run Maintenance

Figure 58. Maintenance Options

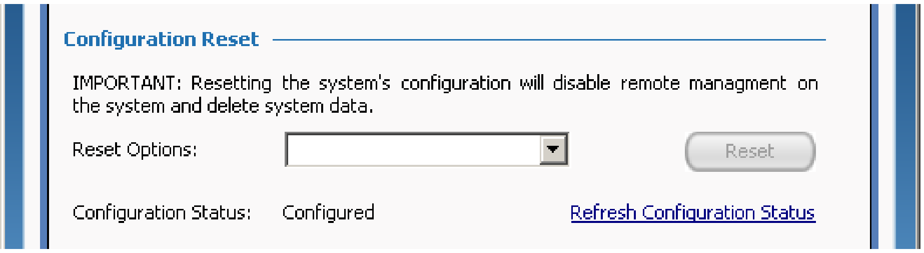
You can run maintenance on a single system (from the Advanced Configuration tab) or on all systems in a collection (see "Performing Operations on a Collection" on page 94).

To manually run maintenance operations:

1. Select the check boxes of the maintenance tasks you want to perform (system time and random admin passwords are always updated):
   - **Re-issue certificates** — Re-issue PKI certificates that are close to the expiry date.
   - **Change AD password** — Change the passwords of the ADOU objects representing the Intel AMT systems.
2. Click **Run Maintenance**. The maintenance operations are performed.

Resetting Configuration of Intel AMT Systems

The Configuration Reset options enable you to reset the configuration of Intel AMT systems.


Configuration Reset

IMPORTANT: Resetting the system's configuration will disable remote managment on the system and delete system data.

Reset Options:

Configuration Status: Configured

Figure 59. Configuration Reset Options

You can perform configuration reset of a single system (from the Advanced Configuration tab) or all systems in a collection (see “Performing Operations on a Collection” on page 94).

To reset configuration:

1. From the Reset Options drop-down list, select one of the following:
   - **Reset configuration** — Removes the configuration settings from the system and disables the Intel AMT features on the system. The system and the Intel SCS can still communicate since the PID, PPS, admin ACL settings, host name, domain name, and the Intel SCS IP and port number are not deleted. Note that if the OEM defined the SOL and IDE interfaces to be closed by default, then a Reset configuration operation will close them and they cannot be reopened without physical access to the MEBx. This is a known Firmware limitation.
   - **Reset to factory defaults** — Deletes all the Intel AMT setup and configuration settings from the system and disables the Intel AMT features on the system.
2. Click **Reset**. A confirmation message appears describing the action you selected. If you are sure that you want to perform the task, click **OK** and then click **OK** again to close the second confirmation message that appears.(If the network interface of the Intel AMT is still open you can send the configuration request from the Console or the Activator utility. If not, you must send the configuration request from the Activator utility.)

Note:

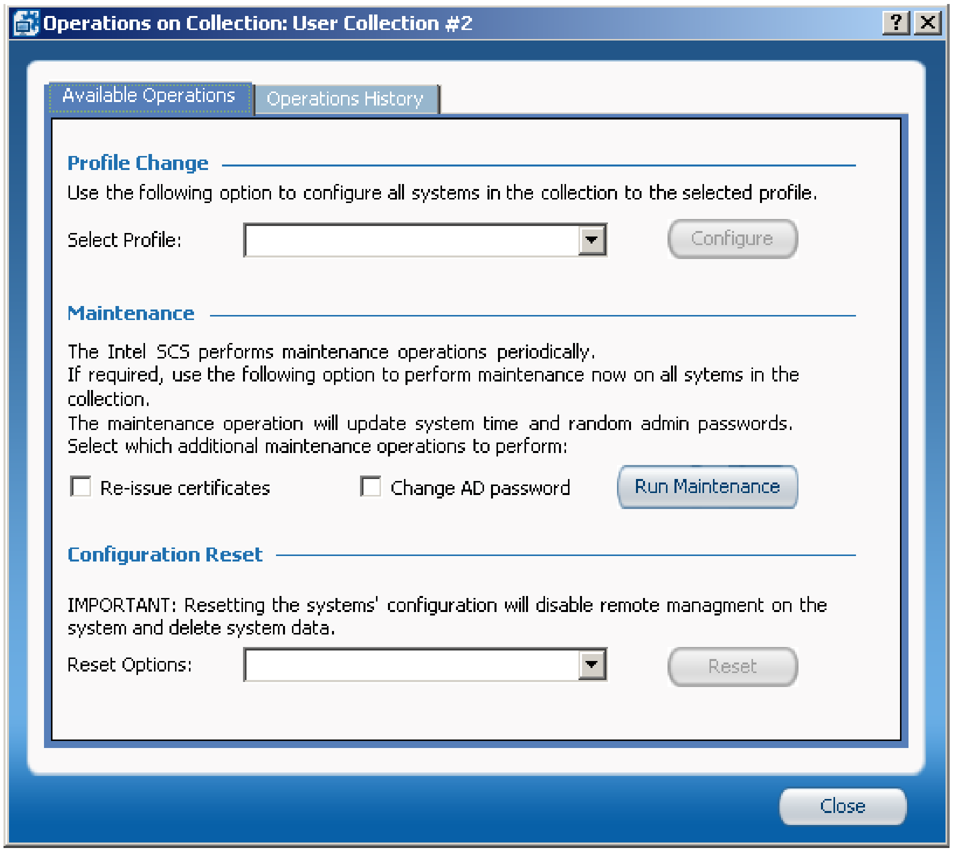
- If auditing was enabled on the Intel AMT system, you cannot reset the configuration unless the auditor has permitted configuration reset.
- The Reset to factory defaults option also deletes any root certificate hashes that were entered manually into the Intel AMT system’s MEBx.

Performing Operations on a Collection

The Console enables you to perform certain operations on all systems in a collection. You can also view the status of each type of operation on each of the systems in the collection.

To view/perform operations on a collection:

1. From the Console tree, right-click the required collection and select **Collection Operations**. The Operations on Collections window appears.



Profile Change

Use the following option to configure all systems in the collection to the selected profile.

Select Profile:

Maintenance

The Intel SCS performs maintenance operations periodically.
If required, use the following option to perform maintenance now on all sytems in the collection.
The maintenance operation will update system time and random admin passwords.
Select which additional maintenance operations to perform:

□ Re-issue certificates □ Change AD password

Configuration Reset

IMPORTANT: Resetting the systems' configuration will disable remote managment on the system and delete system data.

Reset Options:

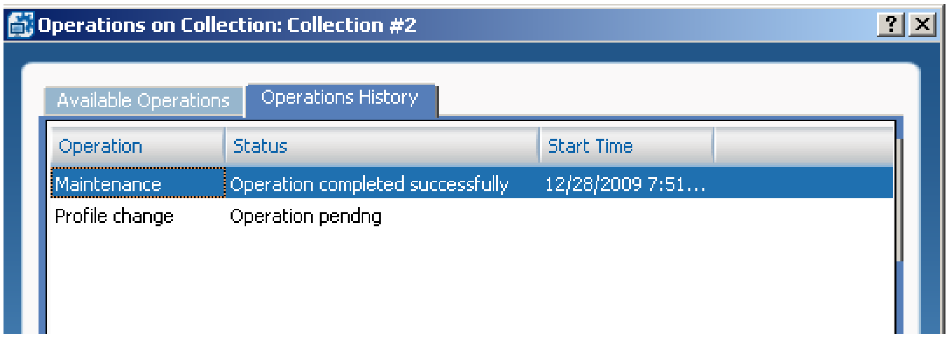
Figure 60. Operations on Collection Window

2. To change the configuration profile: From the Select Profile drop-down list, select the required configuration profile and click **Configure**. All Intel AMT systems in the collection will be reconfigured with the selected profile.

3. Select the options in the following sections to perform the required operations on all systems in the collection:

   - **Maintenance** — See “Manually Run Maintenance Operations” on page 92.
   - **Configuration Reset** — See “Resetting Configuration of Intel AMT Systems” on page 93.

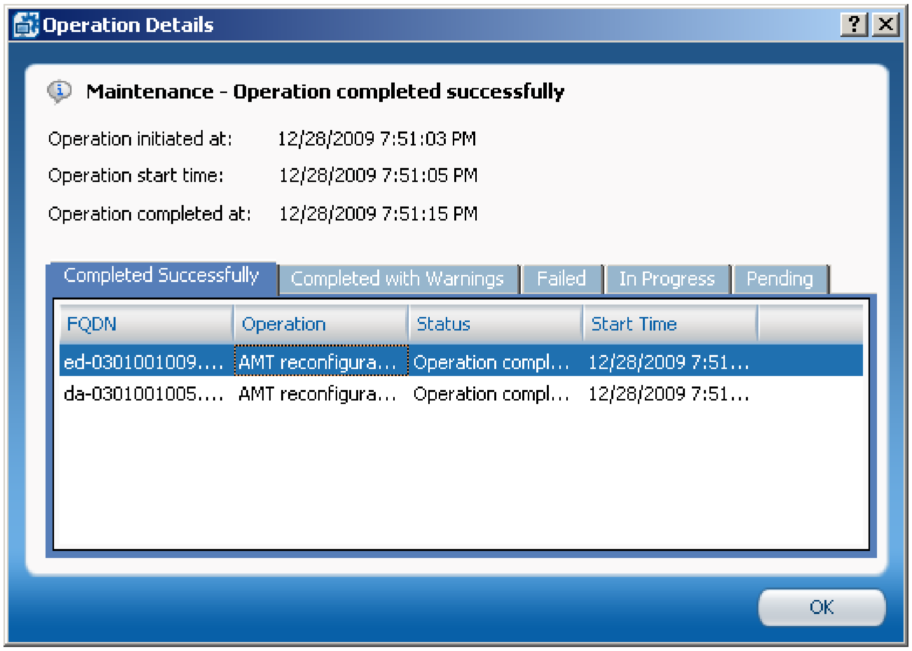
4. To view the status/history of the collection operations, click the **Operations History** tab. The Operations History tab appears.



Operation	Status	Start Time
Maintenance	Operation completed successfully	12/28/2009 7:51…
Profile change	Operation pendng	

Figure 61. Operations History Tab

5. To view details about an operation, double-click the required operation. The Operation Details window appears.



Maintenance - Operation completed successfully

Operation initiated at: 12/28/2009 7:51:03 PM

Operation start time: 12/28/2009 7:51:05 PM

Operation completed at: 12/28/2009 7:51:15 PM

FQDN	Operation	Status	Start Time
ed-0301001009.…	AMT reconfigura…	Operation compl…	12/28/2009 7:51…
da-0301001005.…	AMT reconfigura…	Operation compl…	12/28/2009 7:51…

Figure 62. Operation Details Window

The Operation Details window displays a detailed record for each of the systems that were part of the collection when this operation was performed. The records are displayed in one of the following tabs, according to the status:

- Completed Successfully
- Completed with Warnings
- Failed
- In Progress
- Pending

8

Viewing the Intel SCS Events

This chapter describes how to view the events that the Intel SCS generates.

It includes the following topics:

- About Events and Event Collections
- Viewing Event Details
- Creating an Event Collection
- Exporting Events to a Log File

About Events and Event Collections

All actions performed by users in the Consoles, and all actions performed by the Services, are recorded as events in the database. The Console enables you to group the events into collections (see “Creating an Event Collection” on page 98). The events and event collections are displayed in the *Event Collections* node of the Console tree. (The Console GUI displays a maximum of 1000 events per collection.)

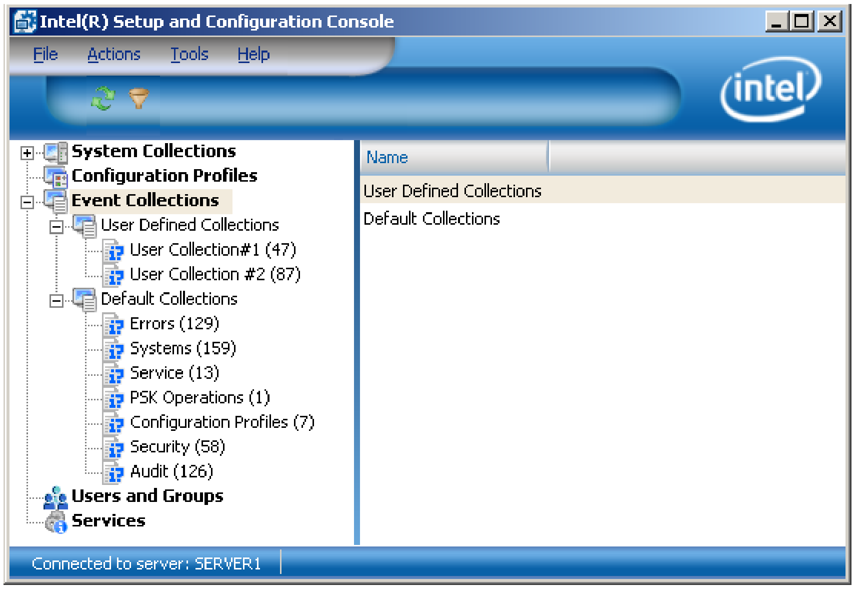


Figure 63. Event Collections Node

The Console includes several default event collections, described in the following table.

Table 15. Default Event Collections

Event Collection	Description
Errors	All operations that failed, are unauthorized, or rejected
Systems	All operations and actions performed on systems
Service	All events related to the service that do not involve configuration
PSK Operations	All events related to TLS-PSK configuration keys
Configuration Profiles	All events related to configuration profiles
Security	All events marked as security related
Audit	All informational events

Note: You cannot edit or delete the default event collections.

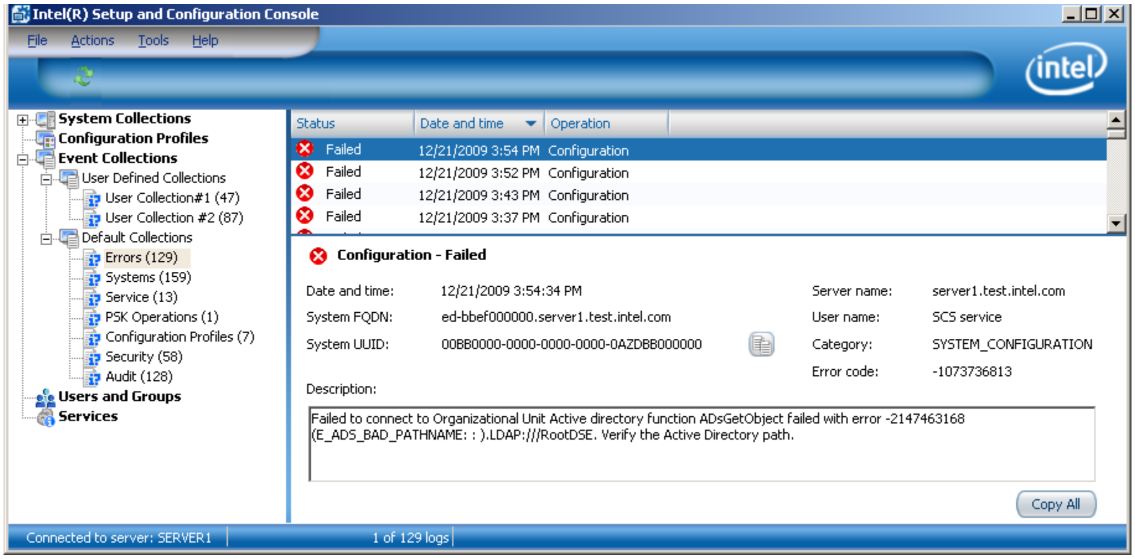
The following table describes the actions you can perform from the Event Collections node:

Table 16. Event Collections Node Actions

Action	How to...
View event details	See “Viewing Event Details” on page 98
Create an event collection	See “Creating an Event Collection” on page 98
Edit an event collection	Right-click the collection and select **Edit Event Collection**
Delete a collection	Right-click the collection and select **Delete Event Collection** (Deleting a collection does not delete the events in the collection.)
Clone and edit a collection	Right-click a default collection and select **Clone and Edit Collection**. The new event collection appears in the *User Defined Collections* node.
Export logs to a log file	See “Exporting Events to a Log File” on page 101
Refresh the list of events in a collection	• Right-click the collection and select Refresh • From the toolbar, click 🔄

Viewing Event Details

When you click a collection in the left pane, the events in that collection appear in the right pane. As you select events in the right pane, the details of the selected event appear in the bottom section of the right pane.



Status	Date and time	Operation
Failed	12/21/2009 3:54 PM	Configuration
Failed	12/21/2009 3:52 PM	Configuration
Failed	12/21/2009 3:43 PM	Configuration
Failed	12/21/2009 3:37 PM	Configuration

Configuration - Failed

Date and time:	12/21/2009 3:54:34 PM	Server name:	server1.test.intel.com
System FQDN:	ed-bbef000000.server1.test.intel.com	User name:	SCS service
System UUID:	00BB0000-0000-0000-0000-0AZDBB000000	Category:	SYSTEM_CONFIGURATION
		Error code:	-1073736813

Description:

Failed to connect to Organizational Unit Active directory function ADsGetObject failed with error -2147463168 (E_ADS_BAD_PATHNAME: :).LDAP:///RootDSE. Verify the Active Directory path.

Figure 64. Event Details Example

Note: You can copy and paste the following information from the event details (via the clipboard):

- Copy the Intel AMT system’s UUID by clicking 📋.
- Copy the event details by clicking **Copy All**.

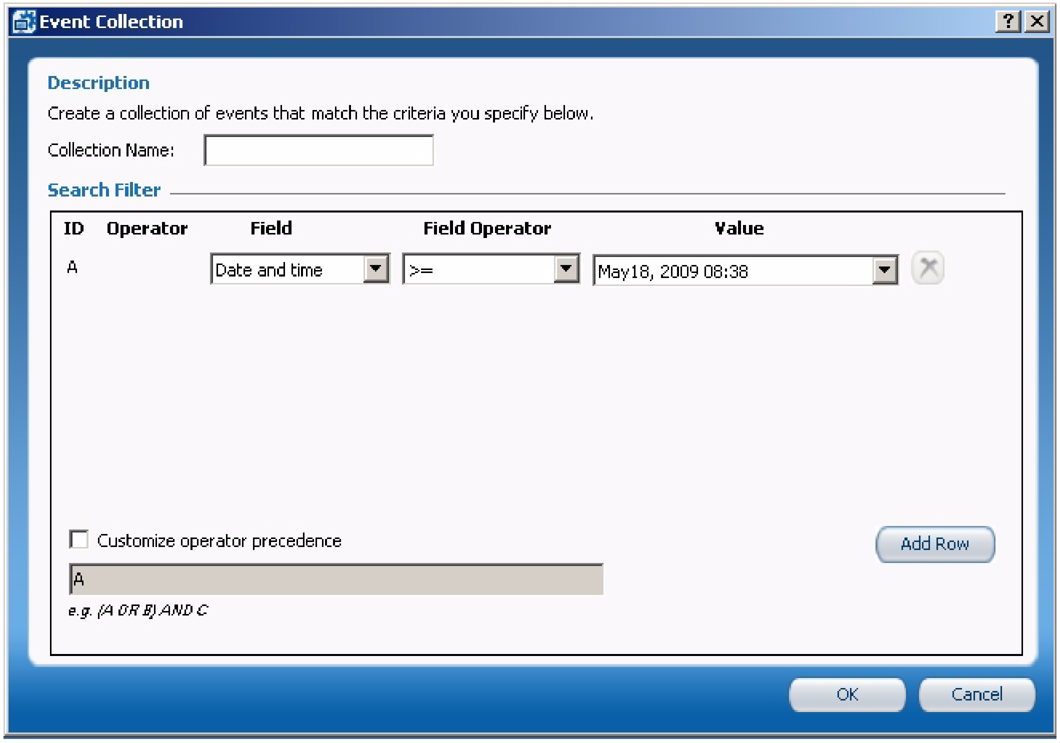
Creating an Event Collection

The Console enables you to create multiple logical groups of events, called event collections, based on filter conditions that you define.

To create an event collection:

1. From the Console tree, select **Event Collections** and perform one of the following:
   - Right-click and select **Create Event Collection**
   - From the toolbar, click ▽ or select **Actions** > **Create Event Collection**

   The Event Collection window appears.



Event Collection

Description

Create a collection of events that match the criteria you specify below.

Collection Name:

Search Filter

ID	Operator	Field	Field Operator	Value
A		Date and time	>=	May18, 2009 08:38

□ Customize operator precedence

A

e.g. (A OR B) AND C

Figure 65. Event Collection Window

2. In the Collection Name field, enter a descriptive name for this collection.

3. Define the filter condition in row A as described in the following table.

Table 17. Event Filter Options

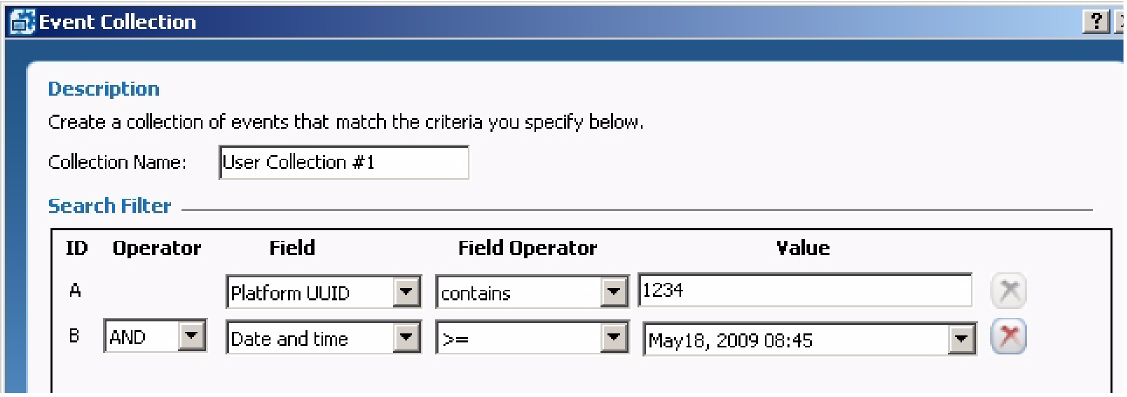
Field	Field Operator	Value
Date and time	• >= • <	By default, the current date and time is displayed in the Value field of these options. You can edit the value directly in the field or click the drop-down list arrow to select a date from a calendar.
Operation Status	in	From the drop-down list, select one or more of the following (hold down the <Ctrl> or <Shift> keys during selection): • **Started** • **Succeeded** • **Completed with warnings** • **Failed** • **Unauthorized** • **Pending** • **Rejected**

Table 17. Event Filter Options (Continued)

Field	Field Operator	Value
System UUID	• starts with • ends with • contains • equals	A string containing the required part of the system's UUID that you want to include in the filter
Category	in	From the drop-down list, select one or more of the following (hold down the <Ctrl> or <Shift> keys during selection): • **Service** • **System_Configuration** • **System_Operation** • **System_Request** • **System_Data** • **Profile** • **PSK** • **Service_Configuration**
Operation	in	From the drop-down list, select one or more of the operation types (hold down the <Ctrl> or <Shift> keys during selection).
Error Code	=	The number of the error code that you want to include in the filter
Originated by	• starts with • ends with • contains • equals	A string containing the required part of the user name who performed the action that you want to include in the filter
Originated from server		A string containing the required part of the server name that you want to include in the filter
Security Log	equals	From the drop-down list, select one or more of the following: • **True** • **False** You cannot use the Security Log filter on its own. It must be used with at least one other filter condition.

4. Optionally, define more filter conditions:

   a. Click **Add Row**. A new filter condition row appears under the existing rows.



Event Collection

Description

Create a collection of events that match the criteria you specify below.

Collection Name: User Collection #1

Search Filter

ID	Operator	Field	Field Operator	Value
A		Platform UUID	contains	1234
B	AND	Date and time	>=	May18, 2009 08:45

Figure 66. Event Filter Example

   b. From the first drop-down list, select one of the following operators to define the relationship of this filter condition with the other filter conditions:

      - **AND** — Include the system only if this condition and the previous condition are both true
      - **OR** — Include the system if either this condition or the previous condition are true

   c. Define the remaining filter conditions as described in Table 17.

   d. Optionally, repeat steps a through c to add additional filter conditions.

5. Click **OK**. The Event Collection window closes and the event collection appears in the *Event Collections* > *User Defined Collections* node of the Console tree.

Exporting Events to a Log File

The Console enables you to export events from a collection to a Comma Separated Values (CSV) file. Each line in the CSV file corresponds to a row in the database, with each field separated by a comma.

To export events to a log file:

1. From the Console tree, right-click the collection and select **Export Logs**.
   The Save As window appears.
2. Optionally, in the File name field edit the name for the log file. By default, the name of the log file contains the collection name and the date and time it was created.
3. Browse to the location where you want to save the log file and click **Save**. The Save As window closes and the events are saved in the log file.

A

CRL XML Format

The Console can import a Certificate Revocation List (CRL) into a configuration profile. The following 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 00 01"/>
                <cert serialnumber="15-27-82-20-00-00-00-00-00-02"/>
                <cert serialnumber="15278220000000000003"/>
        </uri>
        <uri name="http://corppki/crl/mswww(2).crl">
                <cert serialnumber="15 27 82 20 00 00 00 00 00 04"/>
                <cert serialnumber="15 27 82 20 00 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>
```

B

Remote Configuration

This appendix describes how to setup and use the remote configuration feature.

It includes the following topics:

- About Remote Configuration
- Prerequisites for Remote Configuration
- Intel AMT Versions and Remote Configuration Certificates
- Acquiring and Installing a Vendor Supplied Certificate
- Creating and Installing Your Own Certificate

About Remote Configuration

Remote configuration is a feature added with Intel AMT versions 2.2, 2.6, and 3.0 and later versions. It eliminates the need for IT personnel to manually install a PID/PPS pair to enable setup and depends on the following Intel AMT enhancements:

- **Embedded Hashed Root Certificates** — The Intel AMT system contains one or more root certificate hashes from worldwide SSL certificate providers in the firmware image. When the Intel SCS authenticates to the Intel AMT system, it must do so with a certificate compatible with one of the hashed root certificates.
- **Self-signed Certificate** — The Intel AMT system produces a self-signed certificate that is used to pass its public key to the Intel SCS. The Intel SCS must be configured to accept such a certificate.
- **Limited Network Access** — The Activator opens the network interface of the Intel AMT system to send the configuration request. After 24 hours, the interface automatically closes if the setup and configuration is not completed.
- **One Time Password (OTP)** — (Optional) 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 Intel SCS and sends it to the Intel AMT system. The Intel SCS saves the OTP in the database entry associated with the specific Intel AMT system, and uses it to validate the connection. (To set this parameter, see "Defining Service Settings" on page 36.)

The following remote configuration enhancements are available only from Intel AMT release 3.0 and later releases:

- **Simplified One-Touch** — An IT administrator can enter the Intel SCS FQDN or PKI DNS Suffix via the MEBx menu or with a USB key. The Intel AMT system verifies that the FQDN in the Intel SCS certificate matches the entered value. This feature is also known as Secure DNS since providing an FQDN or PKI DNS Suffix is more secure than depending on DHCP option 15.
- **Bare Metal Setup and Configuration** — 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.)

Prerequisites for Remote Configuration

Before remote configuration begins, the following initial conditions must be met:

- The Service is defined to listen for “Hello” messages (see “Defining Individual Service Settings” on page 37).
- The Intel AMT system 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 computer running the Service is registered with a DNS server accessible to the Intel AMT system with the name “Provisionserver” (or the name defined by the OEM) and is in either the same domain as the system or it is in a domain with the same suffix. (This prerequisite is not required for “Hello” messages sent using the Activator CLI.)
- The Intel AMT system is pre-programmed with at least one active root certificate hash.
- The Activator utility files have been copied to the Intel AMT system (This prerequisite not required when using the Bare Metal feature).
- The computer running the Service 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 system.
    - 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 system (see “Intel AMT Versions and Remote Configuration Certificates” on page 106).

Intel AMT Versions and Remote Configuration Certificates

Intel AMT validates the Intel SCS certificate by comparing a domain suffix or FQDN against the CN in the certificate. Different Intel AMT versions perform this comparison in different ways. This can have an impact on the certificate that an organization acquires. If your network includes a mixture of Intel AMT versions, you must acquire a certificate that is appropriate for all the versions that will be configured.

Intel AMT Version 2.2

Intel AMT retrieves its domain suffix using DHCP Option 15. The CN in the Intel 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**.

Intel AMT Version 2.6

Version 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.
- Version 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.

Intel AMT Version 3.0 and Later

If an Intel AMT version 3.0 or later depends exclusively on the domain suffix returned by DHCP, it behaves the same as version 2.2.

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

- If you enter the FQDN of the computer running the Service 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.co**m or ***.corp.yourenterprise.com**.

- If a DNS 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**).

Acquiring and Installing a Vendor Supplied Certificate

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 system vendor. Go to the vendor's website and purchase 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 "Prerequisites for Remote Configuration" on page 105 (the OU is the usual value entered when purchasing a certificate commercially).
- The CN must match the Intel AMT system domain suffix (see "Intel AMT Versions and Remote Configuration Certificates" on page 106).
- 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.

Installing a Vendor Certificate

You can insert more than one certificate into the certificate store of the user account running the Service *(SCSServer.exe)*. The Intel SCS selects the certificate suitable for the specific Intel AMT system.

To install a certificate in the service users certificate store:

1. On the computer where the Service is installed, log in as the user running the Service.
2. Open a command prompt window, enter *mmc* and press <Enter>. The Microsoft Management Console window appears.
3. If the Certificates plug-in is not installed, perform the following:
   a. Select **File** > **Add/Remove Snap-in**. The Add/Remove Snap-in window appears.

   b. Click **Add**. The Add Standalone Snap-in window appears.

   c. From the list of available snap-ins, select **Certificates** and click **Add**. The Certificates snap-in window appears.

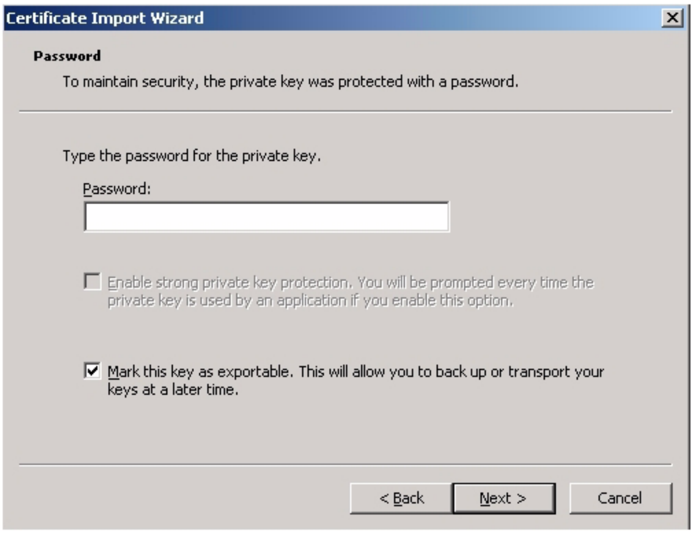
   d. Select **My user account** and click **Finish**. The Certificates snap-in window closes.

   e. Click **Close**. The Add Standalone Snap-in window closes.

   f. Click **OK**. The Add/Remove Snap-in window closes and the Certificates snap-in is added to the Console Root tree.

4. From the Console Root tree, right-click **Certificates > Personal** and select **All Tasks** > **Import**. The Certificate Import Wizard appears.
5. Click **Next**. The File to Import window appears.
6. Enter the path and file name of the certificate to be imported or click **Browse** and navigate to the file.
7. Click **Next**. The Password window appears.

Note: If the **Enable strong private key protection** check box is enabled, ensure that it is NOT selected.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

Figure 67. Certificate Import Wizard

8. Enter the password for the private key.
9. Select the **Mark this key as exportable** check box.
10. Click **Next**.
11. Select **Place all certificates in the following store**. The Personal certificate store should already be selected.
12. Click **Next** and **Finish**.

Installing a Root Certificate and Intermediate Certificates

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 of the computer running the Service *(SCSServer.exe)*.

To save the root certificate:

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, right-click and select **Install certificate**. A certificate manager Import Wizard appears.
3. Click **Next**.
4. Select **Automatically select the certificate store based on the type of the certificate** and click **OK**.
5. Click **Next** then **Finish**.
6. When prompted if you want to add the certificate to the root store, click **Yes**.

Creating and Installing Your Own Certificate

The following sections describe how you can install your own certificate to enable remote configuration:

- Creating a Certificate Template
- Requesting and Installing the Certificate
- Entering a Root Certificate Hash Manually in the AMT Firmware

Creating a Certificate Template

The following procedure describes how to create a remote configuration certificate.

To create the certificate template:

1. From your Certificate Authority server, select **Start** > **Run**. The Run window appears.
2. Enter **mmc** and click **OK**. The Microsoft Management Console window appears.

3. If the Certificate Templates plug-in is not installed, perform the following:

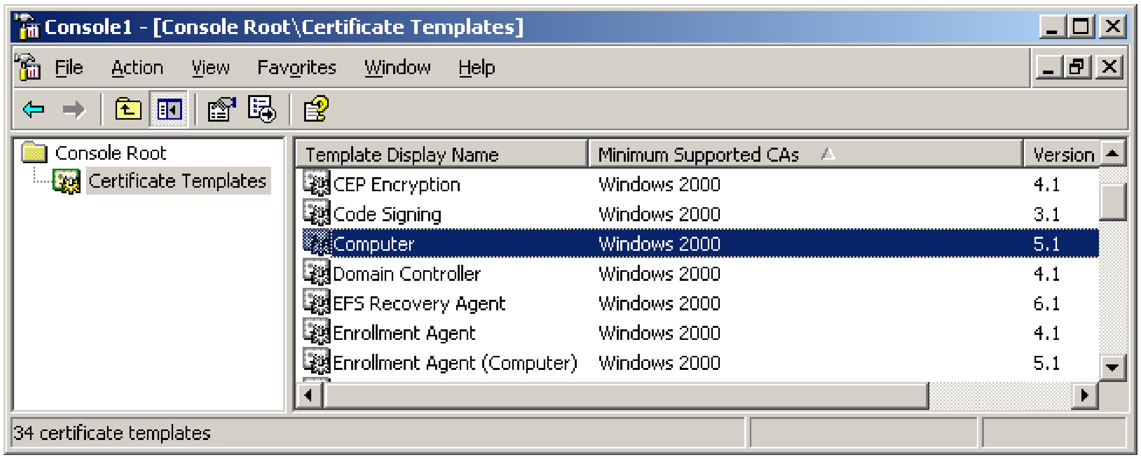
   a. Select **File** > **Add/Remove Snap-in**. The Add/Remove Snap-in window appears.

   b. Click **Add**. The Add Standalone Snap-in window appears.

   c. From the list of available snap-ins, select **Certificate Templates**, click **Add** and then click **Close**. The Add Standalone Snap-in window closes.

   d. Click **OK**. The Add/Remove Snap-in window closes and the Certificate Templates snap-in is added to the Console Root tree.

4. From the Console Root tree, double-click **Certificate Templates**. The list of templates appears in the right pane.



Template Display Name	Minimum Supported CAs	Version
CEP Encryption	Windows 2000	4.1
Code Signing	Windows 2000	3.1
Computer	Windows 2000	5.1
Domain Controller	Windows 2000	4.1
EFS Recovery Agent	Windows 2000	6.1
Enrollment Agent	Windows 2000	4.1
Enrollment Agent (Computer)	Windows 2000	5.1

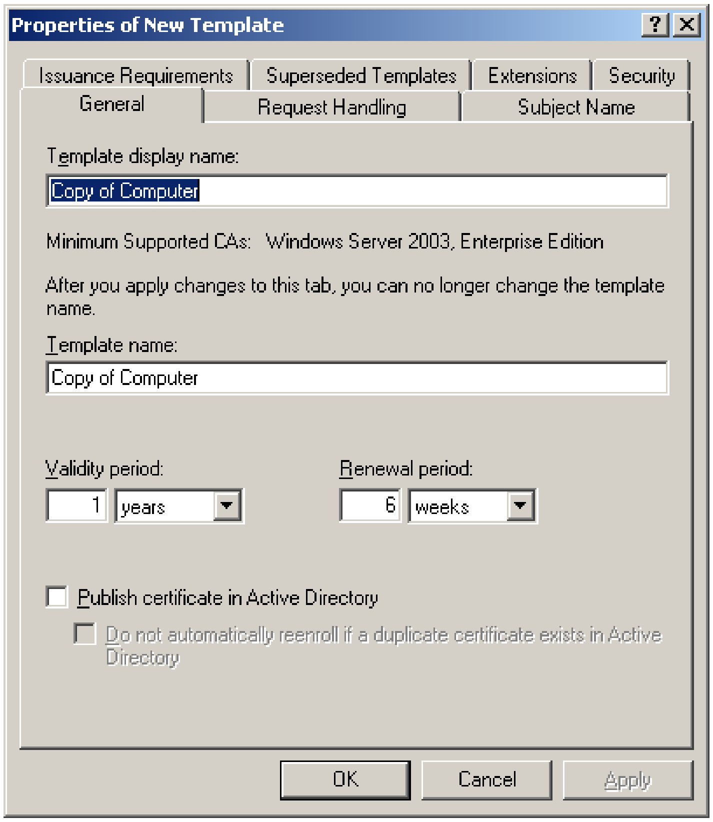
34 certificate templates

Figure 68. Microsoft Management Console

5. In the right-pane, right-click the **Computer** template and select **Duplicate Template**.

> **Note:** If the CA is installed on a server running Windows Server 2008 (all x32/64 versions and R2), the Duplicate Template window appears. Ensure that you select **Windows Server 2003 Enterprise** and click **OK**.

The Properties of New Template window appears.



Template display name: Copy of Computer

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name: Copy of Computer

Validity period: 1 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

Figure 69. Properties of New Template Window

6. In the Template display name field, enter a name for the template.

7. Click the **Extensions** tab. The Extensions tab appears.

8. From the list of extensions, select **Application Policies** and click **Edit**. The Edit Application Policies Extension window appears.

9. Click **Add**. The Add Application Policy window appears.

10. Click **New**. The New Application Policy window appears.

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 select **Supply in the request**.

14. Click the **Request Handling** tab and select the **Allow private key to be exported** check box.

15. Click **OK**. The Properties of New Template window closes.

16. From the Console Root tree, select **Certificate Authority** > **Certificate Templates**.

17. Right-click in the right pane and select **New** > **Certificate Template to Issue**.

18. In the Enable Certificate Templates window, select the template that you just created and click **OK**. The template now appears in the right pane with the other certificate templates.

Requesting and Installing the Certificate

The following procedure describes how to request and install the certificate on the computer running the Service *(SCSServer.exe)*.

To install the certificate:

1. On the computer running the Service, open an internet browser and connect to Certificate Services for the Root CA using the following naming convention **http://CA_FQDN/certsrv**.
2. Click **Request a certificate**.
3. Click **advanced certificate request**.
4. Click **Create and submit a request to this CA**.
5. From the Certificate Template drop-down list, select the certificate template that you created (see "Creating a Certificate Template" on page 109).
6. In the Identifying Information for Offline Template section, enter the domain name where the certificate will be used (the domain suffix or FQDN of the computer running the Service) in the Name field.
7. Leave all the other default values and click **Submit**.
8. Install the certificate in the Service user's certificate store.

Entering a Root Certificate Hash Manually in the AMT Firmware

Normally the certificate hashes are programmed in the Intel AMT system firmware by the OEM. However, there is an option of entering the root certificate's hash manually via the MEBx. (The names and locations of menu options might vary slightly in different Intel AMT Releases.)

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 Intel AMT system and press <Ctrl-P> during boot.
3. When the MEBx menu is displayed, perform a full unprovisioning.
4. From the MEBx menu, select **Setup and Configuration** > **TLS PKI**.
5. Select **Manage Certificate Hashes**.
6. Press <Insert> and enter a name for the hash.
7. Enter the Root certificate thumbprint from step 1.
8. Answer Yes to the question about activating the hash.
9. Exit the MEBx and reboot the Intel AMT system.

C

Certification Authorities and Templates

This appendix describes the Microsoft's Certification Authority (CA) requirements of the Intel SCS and how to define Enterprise CA templates.

It includes the following topics:

- Standalone or Enterprise CA
- Required Permissions on the CA
- Defining Enterprise CA Templates

Standalone or Enterprise CA

The type of CA required by the Intel SCS depends on the features you want to implement.

The following features require a Stand-alone root CA or an Enterprise root CA:

- Transport Layer Security (including Mutual Authentication)
- Remote Access with password based authentication

The following features require an Enterprise root CA:

- Remote Access with certificate based authentication
- 802.1x setups (Wired or WiFi)
- EAC settings

Required Permissions on the CA

The following permissions are required on the CA by the user account running the Service *(SCSServer.exe)*:

- *Issue and Manage Certificates*
- *Request Certificates*

For an Enterprise root CA you also need to grant the Service user account the *Read* and *Enroll* permissions on the templates you want to select in the configuration profiles.

Defining Enterprise CA Templates

When requesting a certificate from a Stand-alone CA, it is possible to change many of the fields in the certificate request manually. This is not true for an Enterprise CA certificate request. The parameters in a template are largely predefined. This is particularly the case for certificates that the Intel SCS requests automatically for an individual Intel AMT system.

Note: Organizational security policies may determine certain template properties, such as certificate expiration. Adjust the values in the following example to the local policy.

The following procedure describes how to create a certificate template.

To create a certificate template:

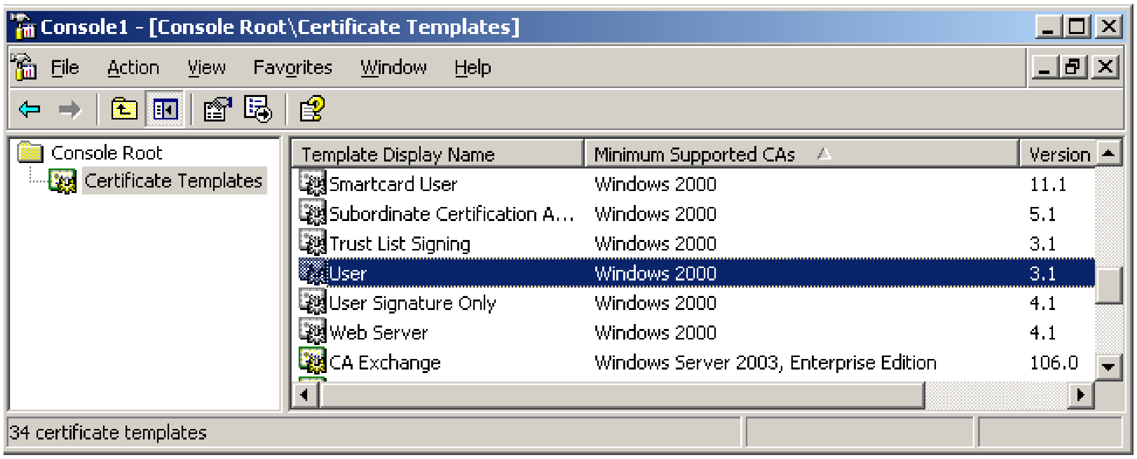
1. From your Certificate Authority server, select **Start** > **Run**. The Run window appears.
2. Enter **mmc** and click **OK**. The Microsoft Management Console window appears.
3. If the Certificate Templates plug-in is not installed, perform the following:

   a. Select **File** > **Add/Remove Snap-in**. The Add/Remove Snap-in window appears.

   b. Click **Add**. The Add Standalone Snap-in window appears.

   c. From the list of available snap-ins, select **Certificate Templates**, click **Add** and then click **Close**. The Add Standalone Snap-in window closes.

   d. Click **OK**. The Add/Remove Snap-in window closes and the Certificate Templates snap-in is added to the Console Root tree.
4. From the Console Root tree, double-click **Certificate Templates**. The list of templates appears in the right pane.



Template Display Name	Minimum Supported CAs	Version
Smartcard User	Windows 2000	11.1
Subordinate Certification A...	Windows 2000	5.1
Trust List Signing	Windows 2000	3.1
User	Windows 2000	3.1
User Signature Only	Windows 2000	4.1
Web Server	Windows 2000	4.1
CA Exchange	Windows Server 2003, Enterprise Edition	106.0

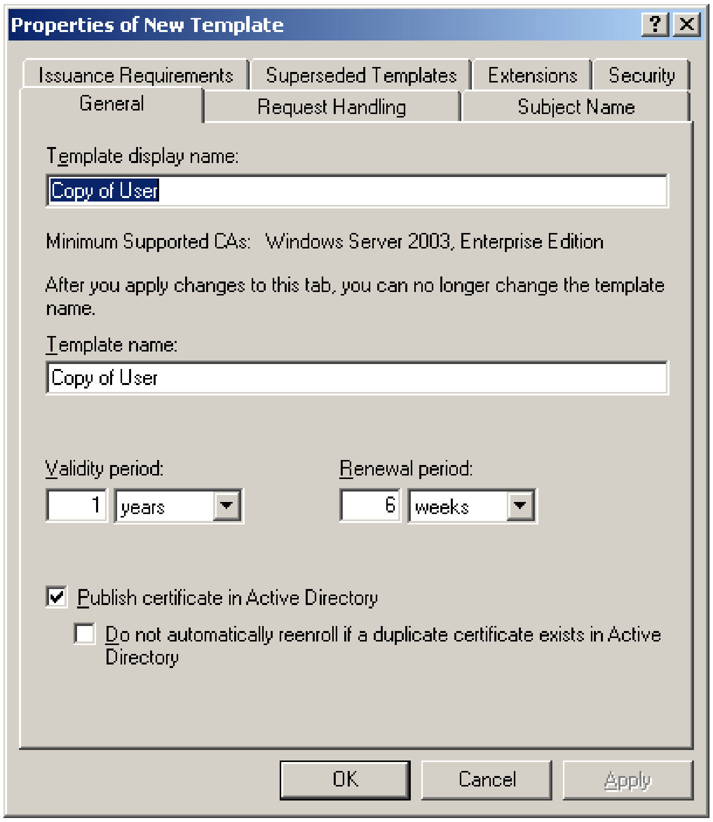
34 certificate templates

Figure 70. Microsoft Management Console

5. In the right-pane, right-click the **User** template and select **Duplicate Template**.

   Note: If the CA is installed on a server running Windows Server 2008 (all x32/64 versions and R2), the Duplicate Template window appears. Ensure that you select **Windows Server 2003 Enterprise** and click **OK**.

   The Properties of New Template window appears.



Template display name: Copy of User

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name: Copy of User

Validity period: 1 years

Renewal period: 6 weeks

☑ Publish certificate in Active Directory

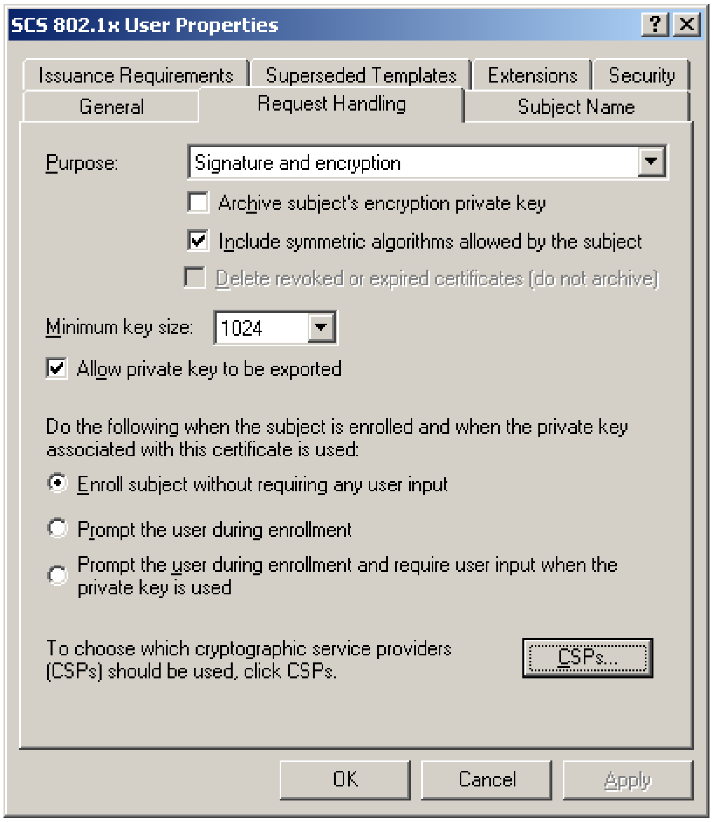
☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

Figure 71. Properties of New Template Window

6. In the Template display name field, enter a meaningful name. For example, name a template used to generate 802.1x client certificates 802.1x.

7. Change the validity and renewal periods as required by local policy and click **Apply**.

8. Click the **Request Handling** tab. The Request Handling tab appears



Purpose: Signature and encryption

□ Archive subject's encryption private key

☑ Include symmetric algorithms allowed by the subject

□ Delete revoked or expired certificates (do not archive)

Minimum key size: 1024

☑ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

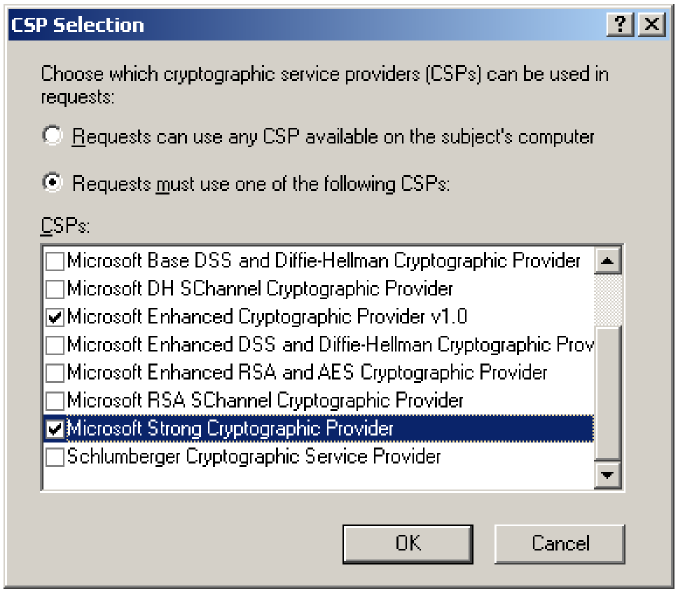
○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs.

Figure 72. Request Handling Tab

9. Click the **CSPs** button. The CSP Selection window appears.



Choose which cryptographic service providers (CSPs) can be used in requests:

○ Requests can use any CSP available on the subject's computer

● Requests must use one of the following CSPs:

CSPs:

□ Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
□ Microsoft DH SChannel Cryptographic Provider
☑ Microsoft Enhanced Cryptographic Provider v1.0
□ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Prov
□ Microsoft Enhanced RSA and AES Cryptographic Provider
□ Microsoft RSA SChannel Cryptographic Provider
☑ Microsoft Strong Cryptographic Provider
□ Schlumberger Cryptographic Service Provider

Figure 73. CSP Selection Window

10. In the list of requests, select the **Microsoft Strong Cryptographic Provider** check box and click **OK**. The CSP Selection window closes.

11. Click the **Subject Name** tab and select **Supply in the request**.
12. Click the **Security** tab. The Security tab appears.
13. Ensure that the user running the Service (or the group the user is in) appears in this list and has the *Read* and *Enroll* permissions.
14. If this is a template for TLS mutual authentication, perform the following:
    1. Click the **Extensions** tab. The Extensions tab appears.
    2. From the list of extensions, select **Application Policies** and click **Edit**. The Edit Application Policies Extension window appears.
    3. Click **Add**. The Add Application Policy window appears.
    4. Click **New**. The New Application Policy window appears.
    5. Enter a policy name, and in the Object Identifier field enter the following OID: **2.16.840.1.113741.1.2.1**
    6. 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.
15. Click **OK**. The Properties of New Template window closes.
16. Select **Start** > **Programs** > **Administrative Tools** > **Certification Authority**.
17. From the Console Root tree, select **Certificate Authority** > **Certificate Templates**.
18. Right-click in the right pane and select **New** > **Certificate Template to Issue**. The Enable Certificate Templates window appears.
19. Select the template that you just created and click **OK**. The Enable Certificate Templates window closes and the template now appears in the right pane with the other certificate templates.