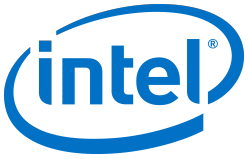


Intel® Setup and Configuration Software (Intel® SCS)

User Guide

Intel® SCS Version: 12.2

May, 2020

License

Intel®Setup and Configuration Software (Intel® SCS) is furnished under license and may only be used or copied in accordance with the terms of that license. For more information, refer to the "Exhibit A" section of the "Intel(R) SCS License Agreement.rtf", located in the Licenses folder.

Legal Information

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

The products described 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.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, specific software, or services activation. Performance varies depending on system configuration. Check with your system manufacturer or retailer.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

Intel® AMT should be used by a knowledgeable IT administrator and requires enabled systems, software, activation, and connection to a corporate network. Intel AMT functionality on mobile systems may be limited in some situations. Your results will depend on your specific implementation. Learn more by visiting Intel® Active Management Technology.

Intel® vPro™ Technology requires setup and activation by a knowledgeable IT administrator. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. Learn more at: http://www.intel.com/technology/vpro.

KVM Remote Control (Keyboard, Video, Mouse) is only available with Intel® Core™ i5 vPro™ and Core™ i7 vPro™ processors with integrated graphics and Intel® Active Management technology activated. Discrete graphics are not supported.

Intel, Intel vPro, and the Intel logo, are trademarks of Intel Corporation in the U.S. and/or other countries.

Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the U.S. and/or other countries.

* Other names and brands may be claimed as the property of others.

Table of Contents

Chapter 1

Introduction

This guide describes how to use Intel® Setup and Configuration Software (Intel® SCS).

This chapter describes Intel SCS and other important background information.

For more information, see:

1.1 What is Intel SCS?

Intel® Setup and Configuration Software (Intel® SCS) is a collection of software components and utilities developed by Intel. You can use Intel SCS to discover, configure, and maintain Intel products and capabilities on the platforms in your network. Intel SCS includes these components:

- **Remote Configuration Service (RCS)** – The RCS is a Windows* based service that runs on a computer in the network. The RCS can process configuration requests sent by the other Intel SCS components. In database mode, the RCS also handles storage of data collected and sent to the RCS by other Intel SCS components.
  For more information, see Setting up the RCS on page 34.
- **Console** – The Console is the user interface to the RCS. You can use the Console to create and edit configuration profiles for supported Intel products and capabilities. In database mode, the Console also lets you view data about Intel products that was sent to the RCS. Database mode also includes additional options for Intel AMT. These options include monitoring Intel AMT systems and creating and running "Jobs" on multiple Intel AMT systems.
  For more information, see Using the Console on page 73.
- **Configurator** – The Configurator (`ACUConfig.exe`) is used to configure Intel AMT (only) and runs locally on each Intel AMT system. You can use the Configurator to configure the system locally or send a configuration request to the RCS.
  For more information, see Using the Configurator on page 126.
- **Intel AMT Configuration Utility** – This utility (`ACUWizard.exe`) is a wizard that you can use to quickly configure individual systems or create XML profiles for host-based configuration using the Configurator. This utility does not interface with the RCS and cannot be used to send requests or data to the RCS. For more information, refer to the `Intel(R)_AMT_Configuration_Utility.pdf`.
- **Remote Configuration Service Utility** – The RCS Utility (`RCSUtils.exe`) is used to do some of the tasks necessary when installing the RCS.
- **Database Tool** – The Database Tool (`DatabaseTool.exe`) is used to do some of the tasks necessary when installing the RCS in database mode. For example, creating the Intel SCS database.
- **Encryption Utility** – The Encryption Utility (`SCSEncryption.exe`) is used to encrypt/decrypt XML files used by Intel SCS.

1.2 What are the Discovery Options?

Intel SCS includes the following methods for discovering data about your platforms.

Discovery Using the Configurator

The Configurator includes a command named `SystemDiscovery`. This command gets data from the Intel AMT device and the host platform of the system. You can save the data in an XML file on the system and/or in the registry. You can also send the data to the database via the RCS (in database mode).

When using this command, you have two options:

- Collect the data (from the XML files or the registry) and add it to your own database using a third-party application. To do this, refer to the documentation of your hardware/software inventory application.
- If you are using the RCS in database mode, you can send the data collected by the Configurator to the Intel SCS database. The data is added to the database record of the system. You can then view this data from the Console.

For the syntax of this command, see Discovering Systems on page 129.

Discovery Using the RCS

When the RCS is installed in database mode, you can also send data discovery queries from the Console. You can send a data discovery query for a single system, or create a job to run a discovery operation on multiple systems. The Console sends a request to RCS to run remote discovery on the specified systems. The RCS uses the WS-Man interface to get the data from the Intel AMT devices. The data retrieved using this method is only saved in the database, and only includes Intel AMT related data. You can then use the Console to view the data collected for each system (see Viewing Discovery Data on page 177).

1.3 What is Intel AMT?

Intel® Active Management Technology (Intel® AMT) lets you remotely access computers when the operating system is not available or the computer is turned off. The only requirement is that the computer must be connected to a power supply and a network.

The Intel AMT environment includes:

- Intel AMT Systems – Computers with an Intel AMT device. The Intel AMT device contains the hardware and software that control the Intel AMT features. The device includes an Intel® Management Engine (Intel® ME) and a BIOS menu called the Intel® Management Engine BIOS Extension (Intel® MEBX). The Intel ME operates independently of the Central Processing Units (CPUs) of the computer.
- Management Console – A software application used to remotely manage computers in a network. The management console must include an interface that can use the features of Intel AMT.

Intel AMT devices are usually supplied in an unconfigured condition. Setup and configuration is the process that gives management consoles access to Intel AMT features. Intel SCS lets you complete this process.

1.4 Configuration Methods and Intel AMT Versions

There are many different versions of Intel AMT. This table gives the configuration methods available for the different Intel AMT versions.

Table 1-1: Configuration Methods

Configuration Method	Intel AMT Versions
Host-based Configuration	6.2 and higher
Remote Configuration using PKI	2.2, 2.6, 3.0 and higher

Note:

Intel ME firmware versions 6.x.x.x – 11.7.x.x having a build number of less than 3000 are considered vulnerable for Intel-SA-00075. (For example, firmware version 9.5.22.1760 would be vulnerable.) It is highly recommended that you upgrade your Intel ME firmware. Read the Public Security Advisory at https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00075.html for more information.

1.4.1 Host-based Configuration

The host-based configuration method is available from Intel AMT 6.2 and higher. This method lets an application running locally on the Intel AMT system configure the Intel AMT device. All configuration is done locally, using the settings in an XML configuration profile (see Defining Intel AMT Profiles on page 86).

Because this method has less security related requirements than earlier configuration methods, by default the Intel AMT device is put in the Client Control mode (see Control Modes on page 15). You can change this setting when you export the profile.

For more information, see:

- Exporting Profiles from the Console on page 83
- Configuring Systems (Unified Configuration) on page 132

Note:

If all your systems have Intel AMT 6.2 and higher, and you do not need to put them in Admin Control mode, you do not need the RCS or Console. Instead, you can use the Intel AMT Configuration Utility. For more information, refer to the `Intel(R)_AMT_Configuration_Utility.pdf`.

1.4.2 Remote Configuration using PKI

The Remote Configuration method uses the Public Key Infrastructure (PKI) of the Transport Layer Security (TLS) protocol and the RCS. To use this method, the Intel AMT device must have at least one active hash certificate defined in the Intel MEBX. If the manufacturer does this before he sends the computer out, then you can configure these computers remotely.

These are the main steps of this configuration method:

1. Prepare the systems and the network for remote configuration (see Setting up Remote Configuration on page 208).
2. Use the Configurator to send a configuration request to the RCS (see Using the Configurator on page 126).

Note:

TLS 1.0 has been deprecated as the security protocol for Intel SCS communication with Intel AMT. The TLS 1.0 protocol has identified security vulnerabilities, including CVE-2011-3389 and CVE-2014-3566. Intel SCS will default to TLS 1.1 or TLS 1.2 (depending on your Intel AMT version) to encrypt communication between Intel SCS software components and Intel AMT. Users can enable TLS 1.0 protocol support for backwards compatibility, both during installation of the Remote Configuration Server (RCS) and after installation/upgrade of the RCS.

1.4.3 Remote Configuration of Mobile Platforms

Remote configuration of Intel AMT (both PKI and PSK) is done Out of Band via the on-board wired LAN interface. This means that mobile platforms can only be configured remotely if both these conditions are true:

1. In addition to the wireless interface, they also have an onboard wired LAN interface.
2. Before configuration starts, the platform is directly connected to your organizations network via the wired LAN interface (not via VPN).

Note:

Some of the latest Intel vPro platforms do not include an onboard wired LAN interface. For information about how to remotely configure these platforms, see Configuration of LAN-less Platforms on the next page.

1.4.4 Configuration of LAN-less Platforms

A LAN-less platform is a system that does not have an on-board wired LAN interface. If you want to configure LAN-less platforms into Client Control mode, you can use the host-based configuration method (or the unified configuration process).

But if you want to configure into Admin Control mode you will need to handle LAN-less systems separately from systems that have an inboard wired LAN interface. This is because, on LAN-less systems, using the remote configuration methods for first configuration of Intel AMT in Admin Control mode will fail. This also means that you cannot use the unified configuration process if you want to configure all systems in Admin Control mode.

This table describes how you can configure LAN-less systems in Admin Control mode.

Table 1-2: LAN-less Versions and Admin Control Mode

Version	How to Configure in Admin Control Mode
Intel AMT 10.x or later	These systems fully support remote configuration. These are the basic steps: 1. Make sure that the correct PKI DNS Suffix for your organization is defined in the Intel MEBX. Remote configuration of these systems requires that this value be pre-defined in the Intel MEBX by the manufacturer/supplier of the Intel AMT system. If it was not pre-defined, you can add it manually in the Intel MEBX. 2. Configure the system locally into Client Control mode. 3. Use the `MoveToACM` command to move the system to Admin Control mode. Although these are the only steps required, it is recommended to configure only basic settings in step #1. Then, after step #2, remotely configure all the remaining required settings. For the recommended procedure, see Remote Configuration of LAN-less Systems below. **Note:** When unconfiguring these systems, do NOT use the `/Full` parameter or the Full Unconfiguration job operation type. Full unconfiguration will delete the PKI DNS Suffix value.

Remote Configuration of LAN-less Systems

1. In the Console, create two profiles specifically for LAN-less systems:
   - A "basic" profile — This profile will be used for local configuration to Client Control mode. These are the only settings that are required in the basic profile:
     - In the Optional Settings window, select the **WiFi Connection** check box and define a WiFi Setup. (Without this WiFi Setup, remote connection to Intel AMT will not be possible after configuration.)
     - In the System Settings window, leave the default settings. But when defining the password for the Intel AMT admin user, make sure that you select only the option named "Use the following password for all systems". Make sure that you define a strong password.
   - A "full" profile — This profile will be used to reconfigure the system with all the settings you want to configure in Intel AMT. Make sure that this profile also includes a WiFi Setup.
2. Select the "basic" profile and then click **Export to XML** to export the profile to an XML file. Make sure that you do NOT select the check box named "Put locally configured devices in Admin Control mode".

3. Use the `ConfigAMT` command of the Configurator to configure the system using the exported XML file. For example:

```
ACUConfig.exe ConfigAMT basicprofile.xml /DecryptionPassword P@ssw0rd
```

   After the command has completed successfully, Intel AMT will be configured in Client Control mode.

4. Use the `MoveToACM` command of the Configurator to move the system to Admin Control mode (see Moving from Client Control to Admin Control on page 143). For example:

```
ACUConfig.exe MoveToACM 192.168.1.10
```

   After the command has completed successfully, Intel AMT will be configured in Admin Control mode.

5. Use the `ConfigViaRCSOnly` command of the Configurator to reconfigure the system using the "full" profile (see Configuring Systems using the RCS on page 134). For example:

```
ACUConfig.exe ConfigViaRCSOnly 192.168.1.10 fullprofile
```

   After the command has completed successfully, the system is configured with all settings that you defined in the full profile. In addition, if you installed the RCS in database mode, the system was added to the database and can be managed using the Console.

1.4.5 Unified Configuration Process

Intel SCS includes a "Unified Configuration" process. This process lets you define one deployment package to configure all Intel AMT versions in your network. Intel SCS automatically uses the necessary configuration method for each Intel AMT device.

The unified configuration process uses two copies of the same profile:

- The first copy is created in the Console. This copy is used by the RCS to remotely configure devices that do not support host-based configuration.
- The second copy is "exported" from the Console and must be included in the deployment package. This copy is used by the Configurator to locally configure devices that support host-based configuration. This copy also includes data (added during export) about the RCS and the required control mode for the Intel AMT device.

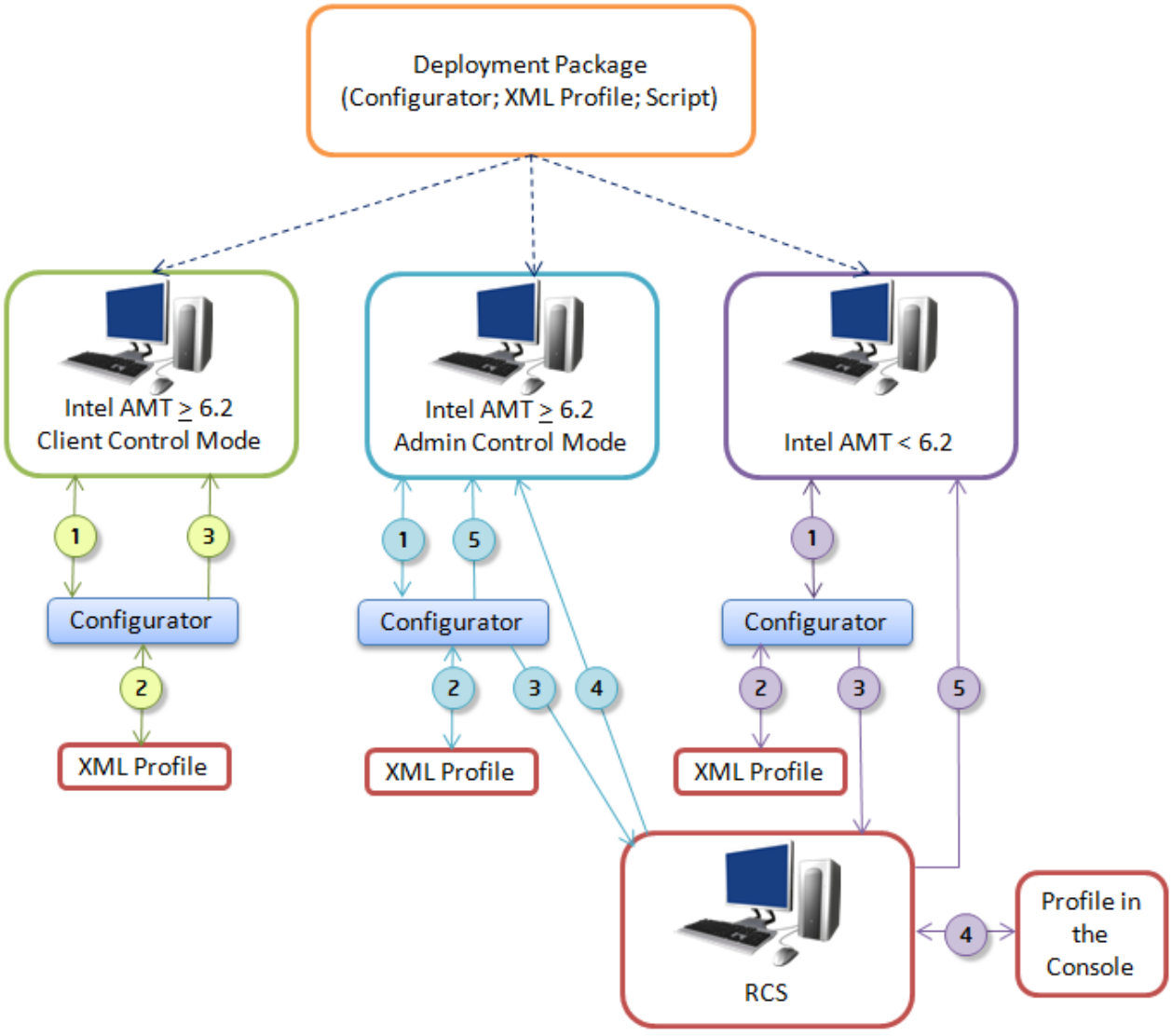


Figure 1-1: Unified Configuration Process

Table 1-3: Steps in the Unified Configuration Process

Step	Description
1 1 1	A script or a batch file runs the Configurator locally on the Intel AMT system. The Configurator examines the Intel AMT device to find if it supports host-based configuration. **Note:** The name of the command to run is `ConfigAMT`. You can also use the unified configuration process to do maintenance tasks using the `MaintainAMT` command. For more information, see: • Configuring Systems (Unified Configuration) on page 132 • Maintaining Configured Systems on page 136
2 2 2	The Configurator examines the settings in the profile sent in the deployment package.
This step occurs if the Intel AMT device supports host-based configuration and "Client Control" mode is defined in the profile:	
3	The Configurator activates Intel AMT on the device and puts the device in Client Control mode. The Configurator uses the local profile to define the settings in the Intel AMT device. All configuration is done locally.
These steps occur if the Intel AMT device supports host-based configuration and "Admin Control" mode is defined in the profile:	
3	The Configurator sends a request to the RCS to "Setup" the Intel AMT device. **Note:** • The device must have a TLS-PSK key or must be configured for remote configuration with PKI. • TLS-PSK Configuration is not supported on Intel AMT 11 or later. • This option is not supported on LAN-less systems (see Configuration of LAN-less Platforms on page 7).
4	The RCS activates Intel AMT on the device and puts the device in Admin Control mode.
5	The Configurator uses the local profile to define the settings in the Intel AMT device. All configuration is done locally.
These steps occur for all Intel AMT devices that do not support host-based configuration:	
3	The Configurator sends a configuration request to the RCS. **Note:** The device must have a TLS-PSK key or must be configured for remote configuration with PKI.

Step	Description
4	The RCS gets the configuration settings from the profile in the Console.
5	The RCS uses the profile in the Console to define the settings in the Intel AMT device. All configuration is done remotely.

1.5 Intel AMT and Security Considerations

This section includes security related topics.

1.5.1 Password Format

Most passwords you define in Intel SCS must be between 8-32 characters, with a minimum of one of each of these:

- A number
- A non alphanumeric character
- A lowercase Latin letter
- An uppercase Latin letter

Note:

- The underscore (_) character is counted as an alphanumeric character.
- The Remote Frame Buffer (RFB) password must be EXACTLY 8 characters long. This password is only used for KVM sessions using port 5900 (see VNC Clients on page 24).
- The colon (:), comma (,), and double quote (") characters are NOT permitted in these passwords:
  - Intel MEBX password
  - Digest user passwords (including the Admin user)
  - RFB password

1.5.2 File Encryption

Configuration profiles created in the Console contain passwords and other data about your network. It is recommended to restrict access to this data. In non-database mode, this data is stored in an encrypted file. In database mode, this data is stored in the SQL database and thus protected by the authentication requirements you define in the SQL Server.

The unified configuration process uses an XML file (exported from a profile in the Console). These XML files can also contain passwords and sensitive data about your network. To protect the data in these files, each profile exported from the Console is encrypted (with a password that you supply).

Some advanced options of Intel SCS use additional XML files (for example, the dedicated network settings file). If you want to use these optional XML files, it is highly recommended to encrypt them. The encryption must be done using the same format used by Intel SCS. To do this, you can use the `SCSEncryption.exe` utility located in the `Utils` folder.

For example:

- To encrypt an XML file named `NetworkSettings.xml`:

  `SCSEncryption.exe Encrypt c:\NetworkSettings.xml <your_password> /output <filename>`

- To decrypt an XML file named NetworkSettings.xml:

  `SCSEncryption.exe Decrypt c:\NetworkSettings.xml <your_password> /output <filename>`

The `/output <filename>` is optional. Without it, SCSEncryption.exe overwrites the input filename with its output.

For more information, refer to the CLI help of the `SCSEncryption.exe` utility.

Notes:

- When encrypting additional XML files, you must use the same password that was used to encrypt the exported profile.
- As of Intel SCS 12.2, the encryption algorithm for `SCSEncryption.exe` has been strengthened. If the XML file was encrypted using the discontinued algorithm, decrypt the file using `SCSEncryption.exe`, then re-encrypt it with `SCSEncryption.exe` to encrypt with the new supported algorithm.

1.5.3 Digital Signing of Files

The executable and DLL files of the Intel SCS components are digitally signed by Intel and include a time-stamp. (This does not include third-party files.) Using digital signatures increases security because it gives an indication that the file is genuine and has not been changed.

The ACU.dll is a library used by the Intel SCS components to do configuration tasks on Intel AMT devices. When running a command from the Configurator CLI, the Configurator tries to authenticate the signature of the ACU.dll. If authentication fails, the task is not permitted and the Configurator returns an error message.

This authentication is also done on external files run by the Configurator. This is the default behavior of the Configurator, but it can be changed per command (see CLI Global Options on page 128). When running CLI commands remotely or in a deployment package, it is not recommended to change this default.

The digital signature is authenticated against a trusted root certificate supplied by AddTrust External CA Root. The time-stamp is authenticated against a trusted root certificate supplied by Commodo. These certificates are located in the user trusted root certificate store of the operating system on the Intel AMT system. The certificates are automatically included in most of the operating system versions supported by the Intel SCS components.

Note:

- Some Windows versions (for example, Windows 8) do not include all of the necessary trusted root certificates. If these systems also do not have access to the Internet, authentication will fail. For more information, see Exit Code 110 on page 219.
- In some environments, authentication of the digital signature can increase the configuration time by up to two minutes

1.5.4 Recommendations for Secure Deployment

Intel recommends these standard security precautions.

Recommendations Related to the Configurator

Intel SCS uses XML files for some of the configuration methods. These XML files can include passwords and data that persons without approval must not access. When using the Configurator and XML files, use these standard security precautions:

- Encrypt all the XML files that the Configurator will use. Use a strong password with a minimum of 16 characters (see File Encryption on page 11).
- Make sure that deployment packages and the encryption password are stored in a location that only approved personnel can access.
- Send deployment packages to the Intel AMT systems with a communication method that prevents access to persons without approval.
- Always use the default requirement for digital signature authentication when using the Configurator CLI remotely (see Digital Signing of Files on page 12).
- If the Configurator will need to communicate with a CA or create an AD object, give permissions only to the specific CA template or the specific Active Directory Organizational Unit.
- XML files created using the Discovery options are not encrypted. Make sure that you delete these files on the Intel AMT systems after collecting the data that they contain.
- When configuration/unconfiguration is complete, delete all files remaining on the Intel AMT system that were used by Intel SCS components.

Recommendations Related to the RCS

If you install and use the RCS, these standard security precautions are also recommended:

- Because installation of any application or service is a sensitive process, always try to run the installer in an isolated environment. In addition, before you run the installer, make sure that the installer file is signed by Intel and that the digital signature is valid.
- The log files saved by the RCS (in the `RCSConfServer` folder) are NOT encrypted. These log files contain data about the network that could be collected and used by an attacker. Make sure that you restrict access to this folder and the logs that it contains.
- The RCS is only as secure as the operating system on which it is running. Make sure that the operating system is always updated with the latest security updates, according to the standards used in your organization for critical resources.
- In database mode, the network connection between the RCS and the database is not secured by Intel SCS. Make sure that this network connection is secured according to the standards used in your organization for critical resources.
- In database mode, the database is only as secure as the RDBMS on which it is installed. Make sure that the RDBMS software is always updated with the latest security updates, according to the standards used in your organization for critical resources.
- When configuring using the Active Directory computer account, RCS will only allow the computer account to un-configure itself, by default, and will reject any attempts by a computer account to un-configure another system's AMT. Note that this restriction does not apply when the user running the configurator is a user account principal.

  This security setting can be disabled in the registry of the system running RCS; however, disabling this feature is not recommended. Data value 1 means that this security setting is enabled. Data value 0 means that this security setting is disabled. This registry setting is found under the following key and value:

  Key: `HKLM\SOFTWARE\WOW6432Node\Intel\Intel(R) Setup and Configuration Software\<version>\RCS\GeneralSettings`

  Value Name: `EnhancedSecurityEnabled`

  Value Type: `REG_BINARY`

  Value Data: `01` (default)

  Note: After changing the registry setting, the RCS service must be restarted for the registry setting changes to take effect.

1.5.5 Control Modes

After configuration, all Intel AMT devices are put in one of these control modes:

- **Client Control Mode** – This mode was added to Intel AMT 6.2 and higher devices. Intel AMT devices in this mode have these security related limitations:
  - The System Defense feature is not available.
  - User consent is required for all redirection operations and changes to the boot process.
  - Permission from the Auditor user (if defined) is not required to unconfigure Intel AMT.
  - To make sure that untrusted users cannot get control of the Intel AMT system, some Intel AMT configuration functions are blocked.
  - During configuration, the Intel MEBX password will not be changed if it is the default password (see Access to the Intel MEBX on page 18).
- **Admin Control Mode** – In this mode all Intel AMT features supported by the Intel AMT version are available.

Note:

By default, the host-based configuration method puts the device in the Client Control mode. All other configuration methods automatically put the device in the Admin Control mode.

1.5.6 User Consent

User consent is a new feature available in Intel AMT 6.0 and higher. If user consent is enabled when a remote connection to a computer starts, a message shows on the computer of the user. The message contains a code that the user must give to the person who wants to connect to his computer. The remote user cannot continue the operation until he supplies this code.

- **Intel AMT 6.x** – The user consent feature is available only for KVM Redirection.
- **Intel AMT 7.x and higher** – For devices in Admin Control mode you can define which operations require user consent. For devices in Client Control mode, user consent is mandatory for these operations:
  - Serial Over LAN to redirect BIOS screens and OS Boot text screens
  - KVM Redirection
  - To remotely set BIOS boot options
  - To change the source for remote boot (for example, boot from PXE)
  - IDE-Redirection (IDE-R) (through AMT 10)

Note: IDE-R is replaced with USB-R in AMT 11.0 and higher

1.5.7 Transport Layer Security Protocol

Transport Layer Security (TLS) is a protocol that secures and authenticates communications across a public network. Intel AMT can use these 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 can use the PSK protocol only before and during the configuration process of Intel AMT systems configured by the RCS. **Note:** TLS-PSK is not supported on Intel® AMT 11 or later.
- **Public Key Infrastructure (PKI)** – The PKI protocol lets users of an unsecured network securely and privately exchange information using an asymmetric public and private cryptographic key pair. The key pair is retrieved and shared through a trusted authority, known as a Certification Authority (CA). The CA supplies digital certificates that can identify an individual or an organization.

These topics include information about how and when these protocols are used:

- Security Before and During Configuration below
- Security After Configuration on the next page

Note:

TLS 1.0 has been deprecated as the security protocol for Intel SCS communication with Intel AMT. The TLS 1.0 protocol has identified security vulnerabilities, including CVE-2011-3389 and CVE-2014-3566. Intel SCS will default to TLS 1.1 or TLS 1.2 (depending on your Intel AMT version) to encrypt communication between Intel SCS software components and Intel AMT. Users can enable TLS 1.0 protocol support for backwards compatibility, both during installation of the Remote Configuration Server (RCS) and after installation/upgrade of the RCS.

1.5.8 Security Before and During Configuration

The host-based configuration method does not send information to the RCS. Configuration is done locally and thus TLS is not necessary and not used. But, to increase security, make sure that the XML files are encrypted (see Recommendations for Secure Deployment on page 14).

Configuration requests sent from an Intel AMT system to the RCS contain security related information about the network environment. Thus, Intel AMT uses one of the TLS protocols (PSK or PKI) before and during the configuration process.

The type of TLS protocol that can be used depends on the version of Intel AMT:

- **Intel AMT 2.1/2.5** – Only support PSK.

  You must change the Intel MEBX password of these Intel AMT systems from the default password. After you install a PSK configuration key and change the password, you must reboot the Intel AMT system.

- **Intel AMT 2.2/2.6/3.x and higher** – Support PSK and PKI.

  To use PKI, the Intel AMT system must have a Root Certificate Hash pre-programmed in the firmware (usually by the manufacturer). You must also install a client certificate on the computer running the RCS.

1.5.9 Security After Configuration

Secure communications between a configured Intel AMT system and a management console depend on the security settings you define in your network.

You can use TLS-PKI in your network to increase the security of communication with all versions of Intel AMT. When TLS is configured (by defining TLS in the configuration profile), communications with Intel AMT are encrypted. If you do not configure TLS, all traffic sent to and from Intel AMT over the network is sent as plain text.

1.5.10 Access to the Intel MEBX

The Intel® Management Engine BIOS Extension (Intel® MEBX) is a BIOS menu extension on the Intel AMT system. This menu can be used to view and manually configure some of the Intel AMT settings. The menu is only displayed if you press a special key combination when the computer is rebooting (usually <Ctrl-P>).

Access to the Intel MEBX is controlled by a password, referred to in this document as the Intel MEBX password. Entry to the Intel MEBX menu for the first time requires a new password to replace the default password (usually "admin").

When an Intel AMT system is configured by the RCS, it is put in the Admin Control mode. In Admin Control mode, if the default password is detected during configuration it is replaced with a password that you define. This new password is defined in the configuration profile.

When a system is configured using the host-based configuration method it is put in the Client Control mode. Client Control mode does not support changing the Intel MEBX password. This means that systems configured in Client Control mode will remain with the default Intel MEBX password (if it is not changed manually).

If you use the Unified Configuration process, you can define the control mode for Intel AMT systems that support host-based configuration. For these systems, the RCS will only replace the default Intel MEBX password if you select this check box when exporting the profile: **Put locally configured devices in Admin Control mode**.

1.6 Admin Permissions in the Intel AMT Device

This section describes how administrator permissions are defined in the Intel AMT device.

Note:

If you lose the passwords of the Intel AMT admin accounts configured in your systems, it may be difficult or impossible to manage or reconfigure Intel AMT on those systems. If the password is lost; you may attempt recovering the password from the monitoring tab of SCS, from the profile used to configure the system, or by reconfiguring the system (some restrictions may stop this method from working properly). Thus, it is highly recommended to define an additional administrator account in Intel AMT (preferably a Kerberos user account). This additional Intel AMT admin account will provide a backup for disaster recovery.

1.6.1 Default Admin User (Digest)

Each Intel AMT device contains a predefined administrative user named "admin", referred to in this guide as the default admin user. Intel AMT uses the HTTP Digest authentication method to authenticate the default admin user.

The default admin user:

- Has access to all the Intel AMT features and settings on the device
- Is not contained in the Access Control List with other Digest users, and cannot be deleted

Thus, for security reasons it is important how you define the password for this user (even if you do not use it). The password is defined in the Network Settings section of the configuration profile (see Defining System Settings on page 119).

These are the methods for defining the password of the default admin user:

Defined Passwords

This method is the easiest method to use and has no prerequisites. But, the password you define in the profile is set in all devices configured with this profile. If the password is discovered, all the devices can be accessed. If you use this method, define a very strong password. To increase security, you can also configure systems with profiles containing different passwords.

Random Passwords

Intel SCS generates a different (random) password for each device. What occurs next depends on the mode that was selected when installing the RCS:

- **Database Mode** – The passwords are saved in the SQL database. You can also use the Console to view the password (see Getting the Admin Password on page 174).
- **Non-Database Mode** – The passwords are not saved. Because the password is not known to you or any application, after configuration you will not be able to connect to the device using the default admin user. Thus, you can only select the random passwords option if the profile contains a Kerberos admin user. For more information, see User-Defined Admin User (Kerberos) on the next page.

Digest Master Password

The RCS calculates a different (unique) password for each device using a secret key (known as the "Digest Master Password") and system-specific data from each device. The RCS does not need to save these admin passwords because they can be recalculated when necessary. After configuration, applications that need to use the default admin user must recalculate the password themselves or ask the RCS to calculate it for them.

Before you can use the Digest Master Password method you need to:

1. Install the RCS (see Setting up the RCS on page 34).
2. Define the Digest Master Password (see Defining the RCS Settings on page 77).

1.6.2 User-Defined Admin User (Kerberos)

If your network has Active Directory (AD), you can also define your own administrative user in the device that will be authenticated using Kerberos. You can then use this user instead of the default admin user.

To use a dedicated Active Directory Admin User (Kerberos):

1. Define an AD user in the Intel AMT device with the PT Administration realm (see Defining the Access Control List (ACL) on page 95).
2. Define a password for the default admin user (see Default Admin User (Digest) on the previous page). The application communicating with the Intel AMT device using the AD user will not use or require this password.
3. Run the Configurator/RCS using the credentials of the user defined in step 1.

Note:

- When using a Kerberos user, always make sure that this Kerberos user exists in the ACL of the profile you use to do reconfiguration.
- When using a Kerberos user and the host-based configuration method:
  - The Configurator must NOT be "Run as administrator".
  - Some reconfiguration and maintenance tasks reset the password of the AD object. If this happens, you must clear the ticket of the Kerberos user before this user can do more configuration operations. You can do this by restarting the Intel AMT system or logging off and on again.

1.7 Maintenance Policies for Intel AMT

After a system is configured, it is recommended to maintain and periodically update the configuration settings in the Intel AMT device. If you do not, your management console might lose connection with the Intel AMT device. For systems where this occurs, the Intel AMT features will not be available from your management console. Also, for increased security, it is recommended to periodically renew the passwords used by Intel AMT. Any password that is not changed regularly causes a risk that it might be discovered by persons without approval. If a password is discovered, it could be used to get access to the system via the Intel AMT device.

It is the responsibility of the network administrator to define and schedule the necessary maintenance tasks for their network environment.

Intel SCS includes two different methods for running maintenance tasks (via "Jobs" or using the CLI). It is recommended to select the method that is best for your network environment, and use only that method.

1.7.1 About Maintenance Tasks

This section describes the main maintenance tasks and when they are necessary.

> **Note:**
>
> The maintenance tasks described in this section are not applicable to systems configured using the Manual configuration method.

Synchronizing the Clock

The Intel AMT device contains a clock that operates independently from the clock in the host operating system. For devices configured to use Kerberos authentication, it is important to synchronize the device clock with the clock of a computer in the network. (The clock of that computer must also be synchronized with the Key Distribution Center. This is not done by Intel SCS.) When the clock is not synchronized, Kerberos authentication with the device might fail.

For Kerberos enabled devices, Intel recommends to synchronize the clock at two week intervals.

Synchronizing Network Settings

After configuration, the Intel AMT device contains IP and FQDN settings that management consoles use to connect to the device. Changes in the network environment or the host operating system might make it necessary to change the settings in the device.

Reissuing Certificates

Intel AMT devices can be configured to use certificates for authentication (when using TLS, EAC, Remote Access, or 802.1x). When certificates are issued by a Certification Authority they are valid for a specified time. These certificates must be reissued before they expire. Intel recommends that you schedule this maintenance task to run a minimum of 30 days before the certificate expiration date.

Replacing Active Directory Object Passwords

If an Intel AMT device is configured to use Active Directory (AD) Integration, an object is created in the AD Organizational Unit specified in the profile. The object contains a password that is set automatically (not user-defined). If the ADOU has a "maximum password age" password policy defined in AD, the password must be replaced before it expires. Intel recommends that you schedule this maintenance task to start a minimum of 10 days before the password is set to expire.

Changing the Default Admin User Password

For increased security, it is recommended to change the password of the default Digest admin user at regular intervals.

Note:

During maintenance, Intel SCS changes the password according to the password method defined in the profile. For more information about these methods, see Default Admin User (Digest) on page 19.

Changing the ADOU Location

If you change the location of the ADOU containing the objects representing the Intel AMT devices, you must reconfigure the systems. This makes sure that all settings that use the object are reconfigured to use the new object.

To change the ADOU location:

1. Define the new ADOU in the configuration profile (see Defining Active Directory Integration on page 92).
2. Use one of these CLI commands to reconfigure the systems:
   - Configuring Systems (Unified Configuration) on page 132
   - Configuring Systems using the RCS on page 134

Note:

Make sure that you include the `/ADOU` parameter with the path to the old ADOU so that Intel SCS can delete the old objects.

1.7.2 Manual/Automatic Maintenance via Jobs

If you installed the RCS component in database mode, you can run maintenance tasks via "jobs". Jobs are run by the RCS, and do not require the Configurator to be sent out to the Intel AMT systems in a deployment package. You can create jobs that do all the specific maintenance tasks that you select, or create jobs that automatically do only the necessary tasks. You can also define recurring jobs that will automatically run according to an interval (of days) that you define.

For more information, see: Managing Jobs and Operations on page 181.

1.7.3 Manual/Automatic Maintenance using the CLI

The Command Line Interface (CLI) of the Configurator includes two commands that you can use to do most of the maintenance tasks. To use this method, you must send the Configurator out to the Intel AMT systems in a deployment package.

These are the CLI commands:

- `MaintainAMT` – See Maintaining Configured Systems on page 136
- `MaintainViaRCSOnly` – See Maintaining Systems using the RCS on page 138

For more information about the Configurator, see Using the Configurator on page 126.

The MaintainAMT and the MaintainViaRCSOnly commands include a parameter named AutoMaintain. You can use this parameter to automate maintenance of Intel AMT systems in your network. This is possible because Intel SCS saves some configuration related data in the registry of each Intel AMT system. The data is updated each time that CLI commands are used to make configuration changes on the system (configuration, reconfiguration, maintenance, and unconfiguration).

The data is saved in this registry key:

- 32-bit operating systems:HKLM\SOFTWARE\Intel\Setup and Configuration Software\SystemDiscovery\ConfigurationInfo
- 64-bit operating systems: HKLM\SOFTWARE\Wow6432Node\Intel\Setup and Configuration Software\SystemDiscovery\ConfigurationInfo

When you use the AutoMaintain parameter:

1. Intel SCS uses the data in the registry to make the decision which maintenance tasks are necessary for each Intel AMT system.
2. Intel SCS automatically does only the necessary tasks that were identified in step 1. If no tasks are necessary, nothing is done.

The following table describes the registry keys and values, and how they are used by the AutoMaintain parameter.

Table 1-4: Keys and Values used by AutoMaintain

Key/Value	Description
Certificates	Contains data of up to three different certificates that were configured in the Intel AMT device. The CertificateExpirationDate key contains the date when the certificate will expire. If there are less than 30 days before one of these expiration dates, reissue all the certificates. (ReissueCertificates task.)
AMTNetworkSettings	Contains data about the network settings configured in the Intel AMT device. The values in the registry are compared with the settings defined in the profile. If they are not the same, the new settings from the profile are configured in the device. (SyncNetworkSettings task.)
String values, located in the root of the ConfigurationInfo key:	
LastRenewAdminPassword	The last time that the password of the default Digest admin user was configured in the Intel AMT device. If this date is more than 6 months old, change the password according to the password setting defined in the profile. (RenewAdminPassword task.)
LastRenewADPassword	The last time that the password was configured in the Active Directory object representing the Intel AMT system. If this date is more than 6 months old, change the password of the Active Directory object. (RenewADPassword task.)

Key/Value	Description
`LastSyncClock`	The last time that the clock of the Intel AMT device was synchronized. If this date is more than 3 months old, synchronize the clock. (`SyncAMTTime` task.) **Note:** The `SyncAMTTime` task is also done every time that one of the other tasks is done.

Note:

- Always run the Configurator under a user that has permissions to create and update these registry keys on the Intel AMT system. The `AutoMaintain` parameter will fail and return an error if it cannot access the registry. Configuration, reconfiguration, maintenance, and unconfiguration tasks will complete but with warnings.
- If the registry keys do not exist, the first time the `AutoMaintain` parameter is used all the maintenance tasks will be done (according to the profile).

1.8 Support for KVM Redirection

Intel AMT 6.0 and higher includes support for third-party applications to operate Intel AMT systems using remote Keyboard, Video and Mouse (KVM) Redirection.

KVM Redirection lets you remotely operate a system as if you are physically located at the remote system. KVM Redirection uses Virtual Network Computing (VNC) to "share" the graphical output of the remote system. The results of keyboard and mouse commands transmitted to the remote system over the network are displayed on the screen of the local system.

VNC includes two main components:

- **VNC Server** – An application located on the remote managed system that permits the VNC Client to connect to and operate the system. From Intel AMT 6.0, a VNC Server component is embedded in the Intel AMT device.
- **VNC Client** – An application, usually located on a management server, used to connect to and operate the remote managed system.

To use KVM Redirection with Intel AMT requires that:

1. KVM is enabled in the Intel MEBX of the Intel AMT system. If disabled in the Intel MEBX, KVM cannot be enabled by Intel SCS during configuration (it must be done manually at the system).
2. The KVM Redirection interface is enabled in the Intel AMT device.
3. A VNC Client is installed on the computer that will control the Intel AMT systems.

VNC Clients

VNC Clients can connect to the VNC Server in the Intel AMT device using these ports:

- **Redirection Ports (16994 and 16995)** – These ports are available to VNC Clients that include support for Intel AMT authentication methods. To use these ports, the VNC Client user must be defined in the Intel AMT device (see Defining the Access Control List (ACL) on page 95). Port 16995 also uses Transport Layer Security.
- **Default Port (5900)** – VNC Clients that do not include support for Intel AMT can use this port. This is a less secure option. To use this port:
  - The VNC Client user must supply the Remote Frame Buffer (RFB) protocol password defined in the Intel AMT device. To define the RFB password, see Defining System Settings on page 119.
  - Port 5900 must be open on the Intel AMT device. Intel SCS does not open this port.

Note:

The VNC Client must use version 3.8 or 4.0 of the Remote Frame Buffer (RFB) protocol.

Chapter 2

Prerequisites

This chapter describes the prerequisites for using Intel SCS to configure Intel AMT.

For more information, see:

2.1 Getting Started Checklist

Before you can use Intel SCS to configure Intel AMT, you will need to collect some data about your network and make some decisions. In many organizations, responsibilities and knowledge about the network is located in several departments. You can print out this checklist and use it as a reference as you collect the necessary data.

Getting Started Checklist for Intel SCS			
1	FQDN	**How is Domain Name System (DNS) resolution done in your network?** On an Intel AMT system, the host platform and the Intel AMT device both have a Fully Qualified Domain Name (FQDN). These FQDNs are usually the same, but they can be different. Intel SCS configures the FQDN of the Intel AMT device. This is one of the most important configuration settings. You must define an FQDN that can be resolved by the DNS in your network. If you do not, after configuration you might not be able to connect to the device. By default, this is how Intel SCS configures the FQDN (hostname.suffix): The hostname part of the FQDN is the hostname from the host operating system. The suffix is the "Primary DNS Suffix" from the host operating system. If this default is not correct for your network, change the setting in the configuration profile. For information about the available settings, see Defining IP and FQDN Settings on page 123.	❑
2	IP	**How does your network assign Internet Protocol (IP) addresses?** On an Intel AMT system, the host platform and the Intel AMT device both have an IP address. These IP addresses are usually the same, but they can be different. Intel SCS configures the IP address of the Intel AMT device. By default, Intel SCS configures the Intel AMT device to get the IP address from a DHCP server. If this default is not correct for your network, change the setting in the configuration profile. For information about the available settings, see Defining IP and FQDN Settings on page 123.	❑
3	Domains	**Do you want to limit access to Intel AMT based on domain location?** Intel AMT includes an option to limit access to the Intel AMT device based on the location of the host system. If you want to use this option, you must define a list of trusted domains. When the host system is not located in one of the domains in the list, access to the Intel AMT device is blocked. The list of domains is defined in the Home Domains window of the configuration profile (see Defining Home Domains on page 99). **Note:** • If you use this option, make sure that you have a complete and accurate list of all the domains where the host system can operate. If you make a mistake when defining this list, you might not be able to connect to the Intel AMT device after it is configured. You must make sure that you always configure systems only with a profile that contains a list of domains correct for those systems. • You must make sure that you define the domain names exactly as they are defined in option 15 of the DHCP servers (on-board specific DNS suffix).	❑

Getting Started Checklist for Intel SCS			
4	VPN	**Do you want to permit access to Intel AMT via a VPN?** By default, Intel AMT devices are configured to block access via Virtual Private Network (VPN) connections. If you want to manage systems outside of the organization's network and are connected to it using VPN, you will need to change this setting. This setting is defined in the Home Domains window of the configuration profile. **Note:** A prerequisite for this setting is to define a list of Home Domains (see item #3 in this checklist).	❑
5	AD	**Do you want to integrate Intel AMT with Active Directory (AD)?** If your network uses AD, you can integrate Intel AMT with your AD. Intel AMT supports the Kerberos authentication method. This means that Intel SCS and management consoles can authenticate with the Intel AMT device using "Kerberos" users. The users are defined in the Intel AMT device using the Access Control List. If integration is enabled, during configuration Intel SCS creates an AD object for the Intel AMT device. Some of the entries in this object define parameters used in Kerberos tickets. Before you can integrate Intel AMT with your AD, you must: • Create an Organizational Unit (OU) in AD 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 component doing the configuration After the OU is created, you must define it in the configuration profile (see Defining Active Directory Integration on page 92).	❑

Getting Started Checklist for Intel SCS			
6	CA	**Does your network use a Certification Authority (CA)?** For these Intel AMT features, a CA is a prerequisite: TLS, 802.1x, EAC, and Remote Access. If you have a CA and want to use these features, this is the data that you need to collect: • Which type of CA do you have? • If you have a Microsoft* CA, which type (Standalone or Enterprise)? • On which operating system is the CA installed? • What is the name and location of the CA in the network? (Will the same CA be used for all Intel AMT features?) • What Common Name (CN) to put in the certificate created for each feature? Intel SCS sends a request to the CA to create certificates. The certificates issued by the CA include CNs. The CNs are defined in the configuration profile for each feature. By default, Intel SCS puts the DNS Host Name in the Subject Name field. In addition, the Subject Alternative Name will include these CNs: DNS Host Name, Host Name, SAM Account Name, User Principal Name, and the UUID of the Intel AMT system. Some RADIUS servers require a specific CN in the Subject Name field. If you need to define a different CN in the Subject Name field, you can do this by selecting the User-defined CNs option for each feature. • How does the CA handle certificate requests? Intel SCS does not support pending certificate requests. This means that the CA must be setup to issue certificates immediately without requiring approval. If you have an Enterprise CA, you must create certificate templates in the CA before you define the profile. For more information, see Defining Enterprise CA Templates on page 192. **Note:** Intel SCS can request certificates from a Microsoft CA or via a CA plugin. For more information, see: • Using Intel SCS with a Microsoft CA on page 192 • Using Intel SCS with the CA Plugin on page 204	❑

Getting Started Checklist for Intel SCS			
7	TLS	**Does your management console require the Intel AMT system to use Transport Layer Security (TLS)?** When TLS is enabled, the Intel AMT device authenticates itself with other applications using a server certificate. 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. TLS is defined in the Transport Layer Security window of the configuration profile (see Defining Transport Layer Security (TLS) on page 107). **Note 1:** A Certification Authority is a prerequisite for TLS (item #6 in this checklist). If using Microsoft CA, the CA can be an Enterprise CA or a Standalone CA. **Note 2:**TLS 1.0 has been deprecated as the security protocol for Intel SCS communication with Intel AMT. The TLS 1.0 protocol has identified security vulnerabilities, including CVE-2011-3389 and CVE-2014-3566. Intel SCS will default to TLS 1.1 or TLS 1.2 (depending on your Intel AMT version) to encrypt communication between Intel SCS software components and Intel AMT. Users can enable TLS 1.0 protocol support for backwards compatibility, both during installation of the Remote Configuration Server (RCS) and after installation/upgrade of the RCS.	❑
8	802.1x	**Does your network use the 802.1x protocol?** If your network uses the 802.1x protocol, you must define 802.1x setups in the configuration profile. If you do not do this, you will not be able to connect to the Intel AMT device after it is configured. If you need to define 802.1x setups, this is the data that you need to collect: • Which 802.1x protocol is used in your network? • Do you want to verify the certificate subject name of the RADIUS Server? You can verify using the FQDN or the domain suffix of the RADIUS server (make a note of the correct value that you want to use). 802.1x is defined in the Network Configuration window of the configuration profile (see Creating 802.1x Setups on page 114). **Note:** These are prerequisites for 802.1x: • Integration with Active Directory (item #5 in this checklist) • A Certification Authority (item #6 in this checklist). If using Microsoft CA, the CA must be an Enterprise CA. • Intel AMT does not support 802.1x when using static IP addresses. This means that both the host operating system and the Intel AMT device must be configured to get their IP address from a DHCP server.	❑

Getting Started Checklist for Intel SCS			
9	EAC	**Does your network use End-point Access Control (EAC)?** If the 802.1x protocol used in your network supports End-Point Access Control (EAC), you can use NAC/NAP authentication with a RADIUS server to authenticate the Intel AMT device. If you need to define EAC, this is the data that you need to collect: • Which authentication method does your EAC vendor use? (NAC, NAP, or NAP-NAC Hybrid.) Note that Intel AMT 9.0 and higher does NOT support NAC. • What is the highest algorithm method supported by your authentication server? (SHA-1, SHA-256, or SHA-384). Note that SHA-256 and SHA-384 are only supported on Intel AMT 6.0 and higher. EAC is defined in the Network Configuration window of the configuration profile (see Defining End-Point Access Control on page 117). **Note:** These are prerequisites for EAC: • Integration with Active Directory (item #5 in this checklist) • A Certification Authority (item #6 in this checklist). If using Microsoft CA, the CA must be an Enterprise CA. • 802.1x (item #8 in this checklist)	❑
10	Remote Access	**Does your network have a Management Presence Server (MPS)?** The remote access feature lets Intel AMT systems located outside an enterprise connect to management consoles inside the enterprise network. The connection is established via an MPS located in the DMZ of the enterprise. **Note:** Intel SCS supports the capability available in Intel AMT to define the MPS. Intel SCS does not ship an MPS and does not endorse or recommend any 3rd party MPS server you may choose to use in your environment. Since Intel SCS cannot perform configuration through an MPS, you must configure your Intel AMT systems on-prem prior to utilizing this capability to manage those systems through the firewall. If you need to define Remote Access, this is the data that you need to collect: • What is the location (FQDN or IP address) and listening port of the MPS? • Do you want to use certificate-based authentication or password-based authentication? Remote Access is defined in the Remote Access window of the configuration profile (see Defining Remote Access on page 100). **Note:** A Home Domain is a prerequisite for Remote Access (item #3 in this checklist).	❑

2.2 Supported Intel AMT Versions

You can use Intel SCS to configure Intel AMT on systems that have Intel AMT 6.2 and higher. Each system that you want to configure using Intel SCS must have these drivers and services installed and running in the operating system:

- **Intel MEI** – The Intel® Management Engine Interface (Intel® MEI) driver, also known as HECI, is the software interface to the Intel AMT device. This driver is usually located under "System devices".
- **LMS** – The Local Manageability Service (`LMS.exe`) enables local applications to send requests and receive responses to and from the device. The LMS listens for and intercepts requests directed to the Intel AMT local host, and routes them to the device via the Intel MEI.

The Intel MEI driver is usually installed by the manufacturer or by running Windows Update on a system, but often the LMS service is not installed. If they are missing, or you need to reinstall them, contact the manufacturer of your system to get the correct versions for your system.

2.3 Supported Operating Systems

This table describes on which operating systems the main Intel SCS components of this release can run.

Table 2-1: Supported Operating Systems

Version	Configurator	RCS	Console
Windows* 10 Pro	Yes	No	No
Windows 10 Enterprise	Yes	No	No
Windows 8.1 Pro	Yes	No	No
Windows 8.1 Enterprise	Yes	No	No
Windows 7 Professional (SP1)	Yes	Yes	Yes
Windows 7 Enterprise (SP1)	Yes	Yes	Yes
Windows Server* 2016	Yes	Yes	Yes
Windows Server 2012 R2	Yes	Yes	Yes
Windows Server 2012	Yes	Yes	Yes
* Other names and brands may be claimed as the property of others.			

Additional Requirements

- The Console works with any 4.x version of Microsoft .NET Framework* (SP1) installed on the computer. This is also true for the wizard version of the Installer used to install the RCS and the Console (`IntelSCSInstaller.exe`), and the Database Tool.
- If you are installing the RCS in database mode, the Microsoft SQL Server Native Client must be installed on the computer. If the client is not installed, the RCS cannot connect to the database. Please refer to www.microsoft.com to find the latest version of this client for the SQL Server version you are running.
- Intel SCS components can run on operating systems installed with these languages: Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Portuguese-Brazilian, Russian, Simplified Chinese, Spanish, Swedish, Traditional Chinese, Turkish.
- For non-English languages, Intel SCS must be installed as a Microsoft Active Directory Service User account with a known password.
- Intel SCS does not support Non-Latin or Extended Latin characters in filenames or values in the XML files.
- A minimum screen resolution of 1024 x 768 is necessary to use the Console. The 800 x 600 screen resolution is not supported.

2.4 Required User Permissions

The permissions required by the user account running the Configurator depend on the state of the Intel AMT device.

Unconfigured Systems

The local user account running the Configurator must have administrator permissions in the operating system. On operating systems with User Account Control (UAC), the Configurator must be "Run as administrator". If the Configurator will be required to request certificates from a Certification Authority (CA), or create Active Directory (AD) objects, the user account must have sufficient permissions to do these tasks.

Configured Systems

After an Intel AMT device is configured, reconfiguration and maintenance tasks can only be done by a user defined in the device with administrator permissions. The user account running the Configurator is not required to have administrator permissions in the operating system.

Note:

If the Intel AMT device is in Client Control mode, you can unconfigure Intel AMT without requiring administration privileges in the device. To do this, you must run the Configurator with a local user account with administrator permissions on the Intel AMT system. On operating systems with (UAC), the Configurator must be "Run as administrator".

Chapter 3

Setting up the RCS

This chapter describes how to set up the Remote Configuration Service.

For more information, see:

3.1 About the RCS

The Remote Configuration Service (RCS) is used to configure remotely and maintain Intel AMT devices. The RCS is a Windows based service (`RCSServer`) that runs on a computer in the network.

You must install and set up the RCS component if you want to do any of these:

- Put Intel AMT devices in the Admin Control mode
- Use the Remote Configuration method
- Use Digest Master Passwords

You do not need the RCS if you want to configure all the Intel AMT devices in your network using only these configuration methods:

- Manual Configuration
- Host-based Configuration on page 5 (in the default Client Control mode)

Note:

Intel SCS does not support multiple instances of the RCS working in the same network environment and connected to the same database.

3.2 Selecting the Type of Installation

The RCS can operate in one of two different modes (defined during installation):

- **Database Mode** – In this mode, data about each Intel AMT system is stored in an SQL database. This includes data that can be used to connect to the system and the admin password that was put in the Intel AMT device. You can then use the Console to monitor the systems and do reconfiguration/maintenance tasks on them.

  To install in this mode, see Installing Database Mode on page 38.

- **Non-Database Mode** – In this mode, the RCS does not store data about the Intel AMT systems. Configuration and maintenance tasks can only be done using the Configurator.

  To install in this mode, see Installing Non-Database Mode on page 48.

3.3 Using the Installer

The Installer (`IntelSCSInstaller.exe`) is located in the RCS folder of the release package. The same file is used to install the RCS in database mode and non-database mode.

You can only install the RCS on computers running an operating system supported by the RCS (see Supported Operating Systems on page 32). You must have local administrator privileges on the computer where you want to install the RCS. To install the RCS on operating systems with User Account Control, you must run the Installer as an administrator.

In addition to the RCS, you can also use the Installer to install a Console. You can install the RCS and the Console on the same computer, or on different computers.

3.4 RCS User Account Requirements

Before starting the installation, you must decide which user account you want to use to run the RCS. (During installation, the Installer does not create the account.)

- If you want to use the built-in Network Service account, it is not necessary to create a user account. This account is more secure, but has some limitations and special considerations (see Using the Network Service Account on the next page).
- If you do not use the Network Service account, create a dedicated user account that will be used only for the RCS. It is NOT recommended to use a group account. You must define a password for this user account, and make sure that you always renew the password before it expires. If the password expires, the RCS will stop working.

When you install the RCS, the Installer will automatically give these permissions to the selected user account:

- Log on as a service permission
- Read permission on the folder containing the `RCSServer.exe` file
- For non-database mode installations only – Read/Write permissions on the folder (`RCSConfServer`) containing the data files used by the RCS (see Location of RCS Log Files on page 54)

(The permissions are given on the computer where the RCS is installed.)

3.5 Using the Network Service Account

The Windows operating system includes a built-in security account named "Network Service". During installation of the RCS, you can select this account to run the RCS. When the RCS runs under this account, the RCS communicates on the network using the credentials of the computer running the RCS. This can increase security because it is not easy for attackers to impersonate a computer.

These sections describe special considerations when using the Network Service account:

Installing Certificates in the Certificate Store

If you want to use the remote configuration method, or configure Mutual TLS, it is necessary to install certificates in the Certificate Store. When using the Network Service account, these certificates must be installed in the certificate store of the Network Service. To do this, you can use the `RCSUtils.exe` utility located in the `Utils` folder.

For example:

```
RCSutils.exe /Certificate Add c:\certificate.pfx P@ssw0rd
```

where `certificate.pfx` is the certificate file in PFX format, and `P@ssw0rd` is the password that was used to encrypt the certificate PFX file.

For more information, refer to the `Intel(R)_SCS_RCSUtility.pdf` also located in the `Utils` folder.

Active Directory and Certification Authority Permissions

Some Intel SCS features and options use the RCS to communicate with the Active Directory or the Certification Authority in your network. Thus, the RCS requires permissions on the AD and the CA. The Network Service is a local account on the computer running the RCS. This means that when you assign these permissions, you must give them to the computer object representing the computer running the RCS.

Installing the Network Service User in Database Mode

In SQL Server, the format used for the Network Service username is different for local and remote connections. If the correct format is not defined, the RCS will fail to connect to the database. The format depends on the location of the RCS and the database:

- If the RCS will be installed on the same computer as the database:

  `"NT Authority\Network Service"`

- If the RCS will NOT be installed on the same computer as the database:

  `"NetBIOS domain name\SAM Account Name"`

  Where the SAM Account Name is the computer where the RCS is installed.

  For example: domain\computer$

When using the `AddUser` command of the Database Tool, you must supply the correct format in the `Username=` parameter. Because the names include spaces, make sure that you enclose the string in quotation marks " ".

3.6 Installing Database Mode

This section describes how to install the RCS in database mode.

Note:

- Before starting the installation, make sure that this is the mode that you require (see Selecting the Type of Installation on page 35)
- If you are installing the RCS in database mode, the Microsoft SQL Server Native Client must be installed on the computer. If the client is not installed, the RCS cannot connect to the database. Please refer to www.microsoft.com to find the latest version of this client for the SQL Server version you are running.

3.6.1 Supported SQL Server Versions

In database mode the data is stored in an SQL database. This table describes on which versions and editions of SQL Server you can install the Intel SCS database.

Version	Enterprise	Standard
Microsoft SQL Server 2016	Yes	Yes
Microsoft* SQL Server* 2014	Yes	Yes
Microsoft SQL Server 2012	Yes	Yes
* Other names and brands may be claimed as the property of others.		

Note:

Intel SCS supports case-sensitive and case-insensitive installations of SQL Server. When installing or upgrading Intel SCS on a case-sensitive version of SQL Server, make sure that you always supply parameter values exactly as they appear in SQL Server. Using incorrect case on a case-sensitive SQL Server installation will cause the installation/upgrade to fail.

3.6.2 Installation Permissions in SQL Server

You can create the Intel SCS database using the Database Tool or the wizard version of the Installer (`IntelSCSInstaller.exe`). You can also use the Database Tool or the Installer to give the RCS permissions on the Intel SCS database. To do these tasks, requires these Server Roles in SQL Server:

- **dbcreator** – Always required (to create the database)
- **securityadmin** – Only required if you want the Database Tool/Installer to create the User and Login ID in SQL Server for the RCS. The User and Login ID are created specifically for the Intel SCS database that you define. They do not have permissions in any other database in SQL Server.

You can also upgrade the Intel SCS database using the Database Tool or the wizard version of the Installer. These are the minimum Database Role Memberships required on the Intel SCS database for upgrade:

- **db_datareader**
- **db_datawriter**
- **db_ddladmin**

During installation/upgrade you have two options for giving the required roles to the Database Tool/Installer:

- **Windows authentication** – Run the Database Tool/Installer with a Windows user account that has the required Server Roles.
- **SQL Server authentication** – When using the Database Tool, use the `Username=` parameter. When using the Installer, you will be asked to supply credentials for SQL Server authentication if Windows authentication fails.

3.6.3 RCS User Permissions in SQL Server

The RCS requires these permissions on the Intel SCS database in SQL Server:

- A User in the Intel SCS database with these Role Member settings:
  - **db_datareader**
  - **db_datawriter**
- An explicit Login ID for the User that is mapped to the Default Schema of dbo

(During installation, the Database Tool/Installer can create the User and the Login ID for you.)

You have two options for how the RCS will connect to the Intel SCS database:

- **Windows authentication** – The RCS will use the credentials of the Windows user account that is running the RCS (`RCSServer.exe`).
- **SQL Server authentication** – The RCS will use the credentials of an SQL Server user. This method of authentication is considered less secure. In addition, the Login ID and password of the SQL Server user are saved in the registry of the computer running the RCS (the password is encrypted).

During installation of the RCS, you must select the authentication method in the Database Settings window of the Installer. When using the Database Tool to add the user to the database, use the `RCSUserWinAuth=` parameter of the `AddUser` command to specify the authentication method.

3.6.4 Creating the Database

In many organizations, the company databases are managed by a database administrator (DBA). Usually, the DBA will want to control how the Intel SCS database is installed. The DBA (or you) can use the Database Tool, located in the RCS folder, to create the database before you install the RCS. The Database Tool (`DatabaseTool.exe`) is a simple CLI that you can use locally on the SQL Server or remotely.

Note:

When complete, the `CreateDB` command creates a storage encryption key file. The file is encrypted with a password that is printed to the screen in the CLI output of the command. Make sure that you save this file and password in a secure location. You will need them later.

This is the syntax and parameters for the `CreateDB` command:

```
DatabaseTool.exe CreateDB DBServer=<DB server> DBName=<DB name>
[Username=<SQL Login ID> Password=<SQL password>] [KeyFileName=<filename>]
```

`DBServer=`	The name (FQDN) or IP address of the SQL Server
`DBName=`	The name of the database
`Username=`	By default, the credentials of the user account running the Database Tool are used to authenticate with SQL Server. If you want the Database Tool to use SQL Server authentication instead, use this parameter to supply the Login ID.
`Password=`	The password of the SQL Server account (only necessary if the user was supplied in the Username parameter)
`KeyFileName=`	By default, the Database Tool creates an encryption key file named `RCSStorage.key` in the folder where the Database Tool is located. You can use this parameter to supply an alternative path and filename.

Examples

Example #1: Creating a database on the local SQL Server:

```
DatabaseTool.exe CreateDB DBServer=(local) DBName=TestDB
```

Example #2: Creating a database on a remote SQL Server:

```
DatabaseTool.exe CreateDB DBServer=192.168.1.10 DBName=TestDB
```

Example #3: Creating a database using SQL Server authentication:

```
DatabaseTool.exe CreateDB DBServer=192.168.1.10 DBName=TestDB Username=MySQLUser
Password=P@ssw0rd
```

3.6.5 Adding the RCS User to the Database

After creating the database, you (or the DBA) must define how the RCS will access the database and which user account it will use. To do this, use the `AddUser` command of the Database Tool.

This is the syntax and parameters for the `AddUser` command:

```
DatabaseTool.exe AddUser DBServer=<DB server> DBName=<DB name>
[Username=<SQL Login ID> Password=<SQL password>]
RCSUserWinAuth=<0|1> RCSUsername=<username> [RCSPassword=<password>]
```

`DBServer=`	The name (FQDN) or IP address of the SQL Server
`DBName=`	The name of the database
`Username=`	By default, the credentials of the user account running the Database Tool are used to authenticate with SQL Server. If you want the Database Tool to use SQL Server authentication instead, use this parameter to supply the Login ID.
`Password=`	The password of the SQL Server account (only necessary if the user was supplied in the `Username` parameter)
`RCSUserWinAuth=`	Defines the type of authentication used by the RCS to authenticate with the database. Valid values: • 0 – SQL Server authentication • 1 – Windows authentication
`RCSUsername=`	The name of the user account to be used by the RCS to authenticate with the database. • If `RCSUserWinAuth=0` – This will be the Login ID used by the RCS during SQL Server authentication. If the Login ID does not exist, it will be created by the Database Tool. • If `RCSUserWinAuth=1` – This will be the Domain user account under which the RCS will run. You must make sure that you specify the same name when you install the RCS (in the Database Settings window). **Note:** If `RCSUserWinAuth=1` and you are using the Network Service account, the format of the username depends on where the RCS and database are located. For more information, see Using the Network Service Account on page 37.
`RCSPassword=`	The password of the user account to be used by the RCS to authenticate with the database. Only necessary if `RCSUserWinAuth=0`.

Examples

Example #1: Adding a user to a database on the local SQL Server:

```
DatabaseTool.exe AddUser DBServer=(local) DBName=TestDB RCSUserWinAuth=1
RCSUsername=MyRCSUser
```

Example #2: Adding a user to a database on a remote SQL Server:

```
DatabaseTool.exe AddUser DBServer=192.168.1.10 DBName=TestDB RCSUserWinAuth=1
RCSUsername=MyRCSUser
```

Example #3: Adding the Network Service user (RCS is local on SQL Server):

```
DatabaseTool.exe AddUser DBServer=192.168.1.10 DBName=TestDB RCSUserWinAuth=1
RCSUsername="NT Authority\Network Service"
```

Example #4: Adding the Network Service user (RCS is connecting remotely):

```
DatabaseTool.exe AddUser DBServer=192.168.1.10 DBName=TestDB RCSUserWinAuth=1
RCSUsername="domain\computer$"
```

Example #5: Adding a user (that will use SQL Server authentication):

```
DatabaseTool.exe AddUser DBServer=192.168.1.10 DBName=TestDB Username=MySQLUser
Password=P@ssw0rd RCSUserWinAuth=0 RCSUsername=MyRCSUser RCSPassword=P@ssw0rd
```

3.6.6 Installing the RCS and Console

This procedure describes how to install the RCS (and Console) in database mode.

Note:

Before starting the installation, make sure that this is the mode that you require (see Selecting the Type of Installation on page 35).

To install in database mode:

1. Double-click `IntelSCSInstaller.exe`. The Welcome window opens.
2. Click **Next**. The License Agreement window opens.

3. Select **I accept the terms of the license agreement** and click **Next**. The Select Components window opens.

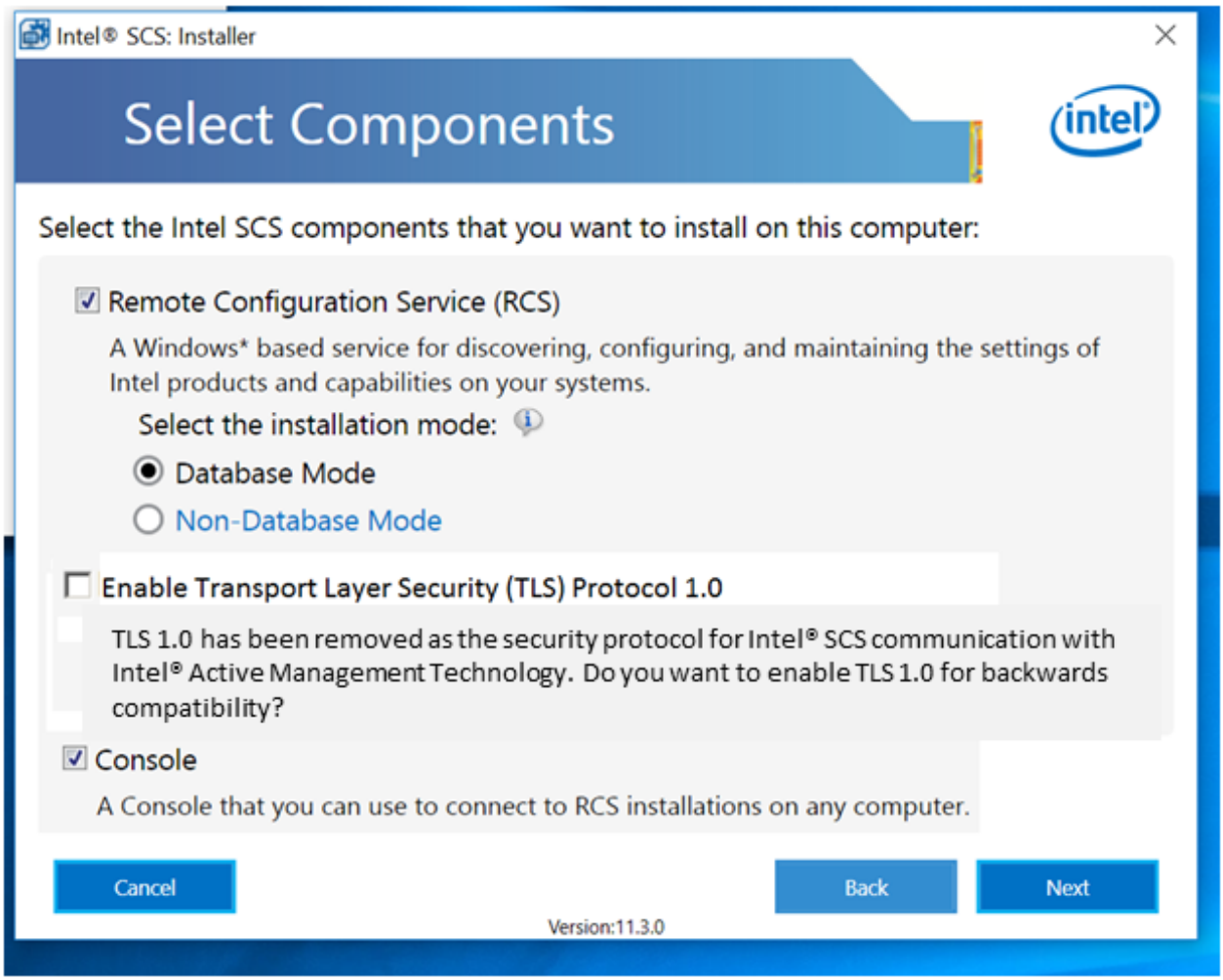


Figure 3-1: Select Components Window

4. Select the check boxes of the components that you want to install on this computer:
   - **Remote Configuration Service (RCS)** – Installs the RCS.

     Note:

     When installing the RCS, make sure that the **Database Mode** option is selected.

   - **Enable TLS 1.0 Protocol for Encryption** – Enables the TLS 1.0 protocol for encryption. Intel SCS defaults to TLS 1.1 or TLS 1.2 (depending on the Intel AMT version of the system being configured) to encrypt communication to Intel AMT. TLS 1.0 has been deprecated as the security protocol for Intel SCS communication with Intel AMT, as the TLS 1.0 protocol has identified security vulnerabilities, including CVE-2011-3389 and CVE-2014-3566.

     Intel SCS allows users to enable TLS 1.0 protocol support for backwards compatibility with legacy Intel AMT platforms. For instructions on how to disable TLS 1.0 protocol support, see Configuring Transport Layer Security (TLS) Protocol Support on page 72.
   - **Console** – Installs the Console. You can install this component on any computer that can connect to the computer running the RCS.
5. Click **Next**. A confirmation dialog box appears. Select **Yes** to confirm that you want to enable TLS 1.0 Protocol support, or select **Cancel** to return to the Select Components window.

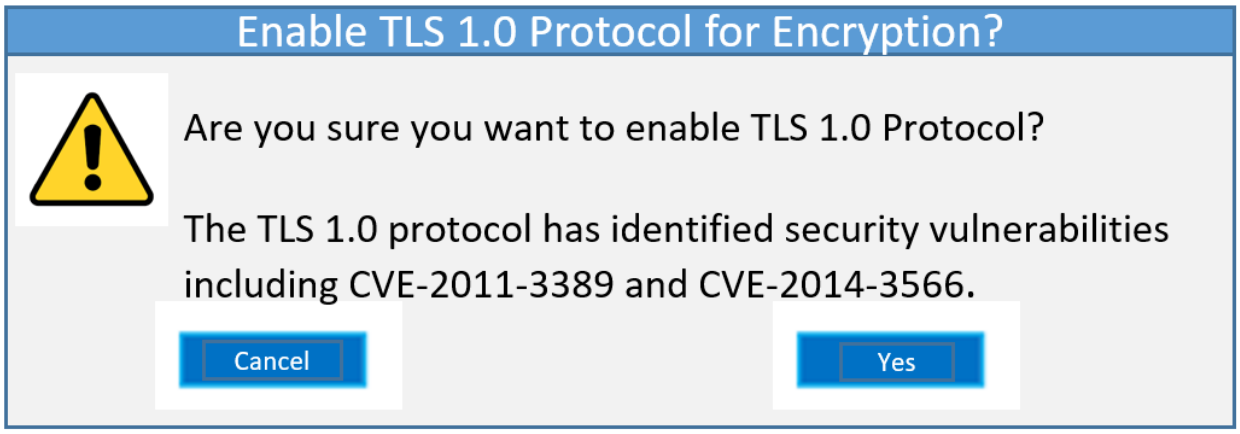


Figure 3-2: TLS 1.0 Enablement dialog box

6. If you selected the option to install the RCS, the RCS User Account window opens. This window defines the user under which the RCS will run.

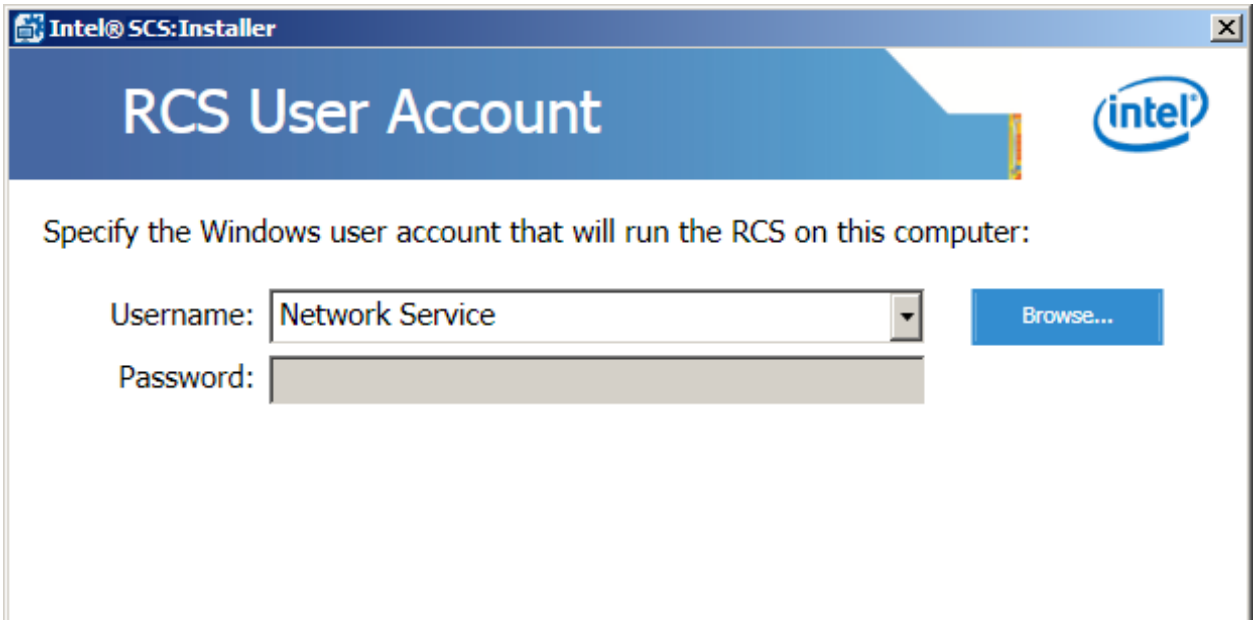


Figure 3-3: RCS User Account Window

> **Note:**
>
> In the Username field, by default, the Network Service account is selected. It is recommended to run the RCS using this built-in security account (see Using the Network Service Account on page 37).

7. (Optional) If you do not want to use the Network Service account:
   a. Click **Browse**. The Select Users or Groups window opens.
   b. Enter the user that will run the RCS on this computer. Enter the username in the format domain\username.
   c. Click **OK**. The Select Users or Groups window closes.
   d. In the Password field, enter the password of the user you selected (only the Network Service account does not require a password).

8. Click **Next**. The Database Settings window opens. This window defines the location of the database and how the RCS will authenticate with the database.

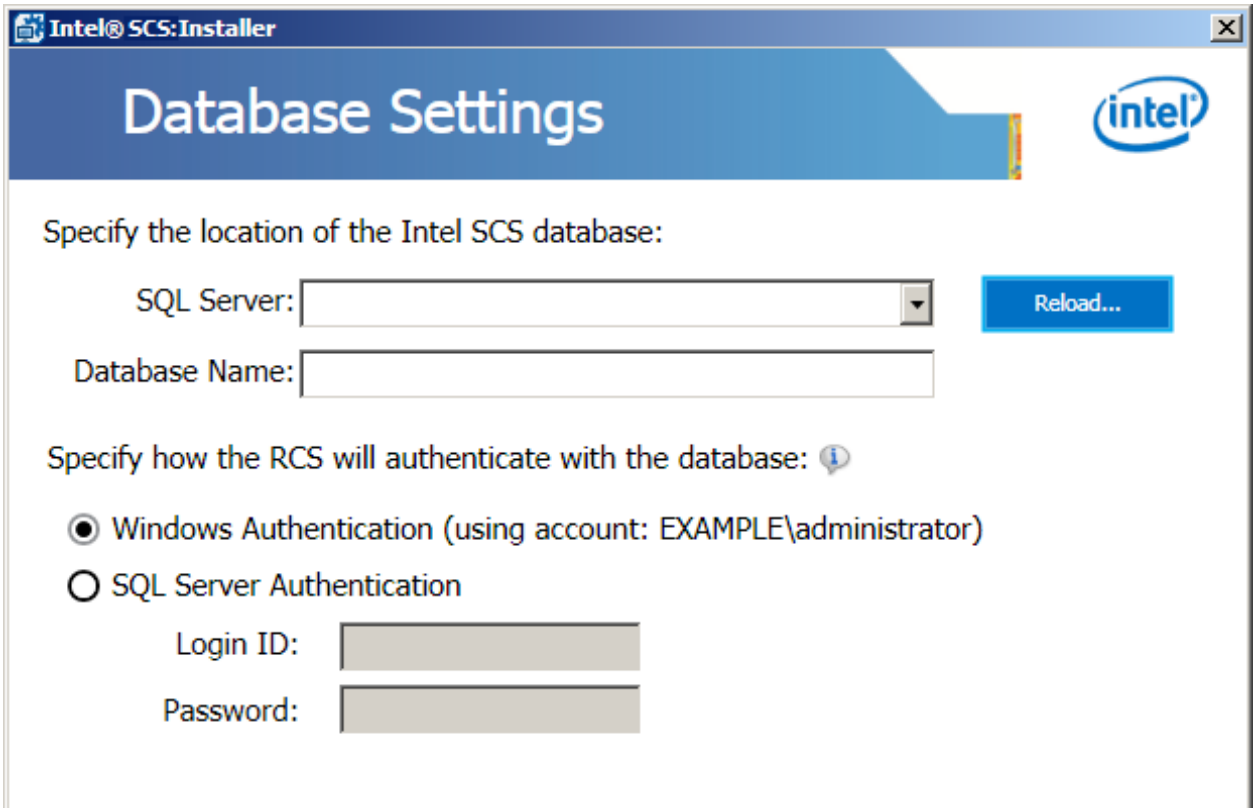


Figure 3-4: Database Settings Window

9. Specify the location of the database:

   a. In the SQL Server field, enter the name of the SQL Server where the Intel SCS database was installed. (If you did not create a database, enter the name of the SQL Server where you want to create the database.)

   b. In the Database Name field, enter the name of the Intel SCS database exactly as it was defined during installation of the database. (If you did not create a database, enter the name of the database that you want to create.)

10. Specify the authentication method that the RCS will use:

    - **Windows Authentication**
    - **SQL Server Authentication** – If you select this option, enter the Login ID and the password of the SQL Server account. The account that you specify MUST have a password. SQL Server authentication using an account without a password is not supported.

    For more information, see RCS User Permissions in SQL Server on page 39.

11. Click **Next**. The Installer will try to connect to the database. If the Installer cannot locate the database a new window named Create Intel SCS Database opens. If this window opens, you have two choices:
    - If you know that the database already exists (because you or the DBA created it using the Database Tool), click **Close** and correct the values you specified in the Database Settings window.
    - If you did not create a database, click **Create Database**. The Installer will try to create the database and also automatically create and install the storage encryption key. If you select this option, follow the instructions in the windows that are shown, and then continue from step 12.
12. If the Installer successfully located the database, the Storage Encryption Key window opens. This window installs the encryption key for the RCS to use when accessing the database.

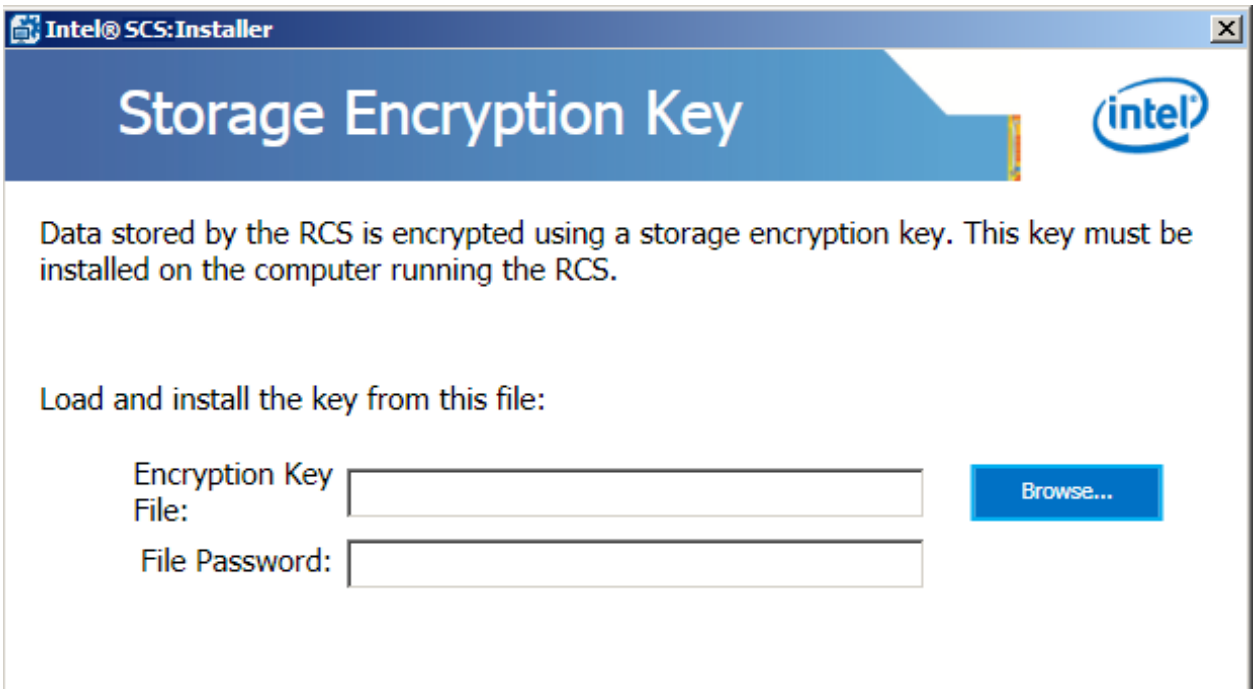


Figure 3-5: Storage Encryption Key Window

13. Click **Browse** and select the storage encryption key file that was created by the Database Tool utility when the database was created. In the File Password field you must also enter the password that was used to encrypt the key file. This is the random password that was shown in the CLI when the `CreateDB` command completed.
14. Click **Next**. The Confirmation window opens. This window shows information about the selections you made.
15. (Optional) The default installation folder is `C:\Program Files (x86)\Intel\SCS12`.

    If you want to change this location, in the Install path field enter a new path or click **Browse** to select it.
16. Click **Install**. The Installation Progress window opens. When installation is complete, a message is shown.
17. Click **Next**. The Completed Successfully window opens.
18. Click **Finish**. The Installer closes. The RCS is installed with default settings. If necessary, you can change these settings (see Defining the RCS Settings on page 77).

3.7 Installing Non-Database Mode

This procedure describes how to install the RCS (and Console) in non-database mode.

Note:

Before starting the installation, make sure that this is the mode that you require (see Selecting the Type of Installation on page 35).

To install in non-database mode:

1. Double-click `IntelSCSInstaller.exe`. The Welcome window opens.
2. Click **Next**. The License Agreement window opens.
3. Select **I accept the terms of the license agreement** and click **Next**. The Select Components window opens.

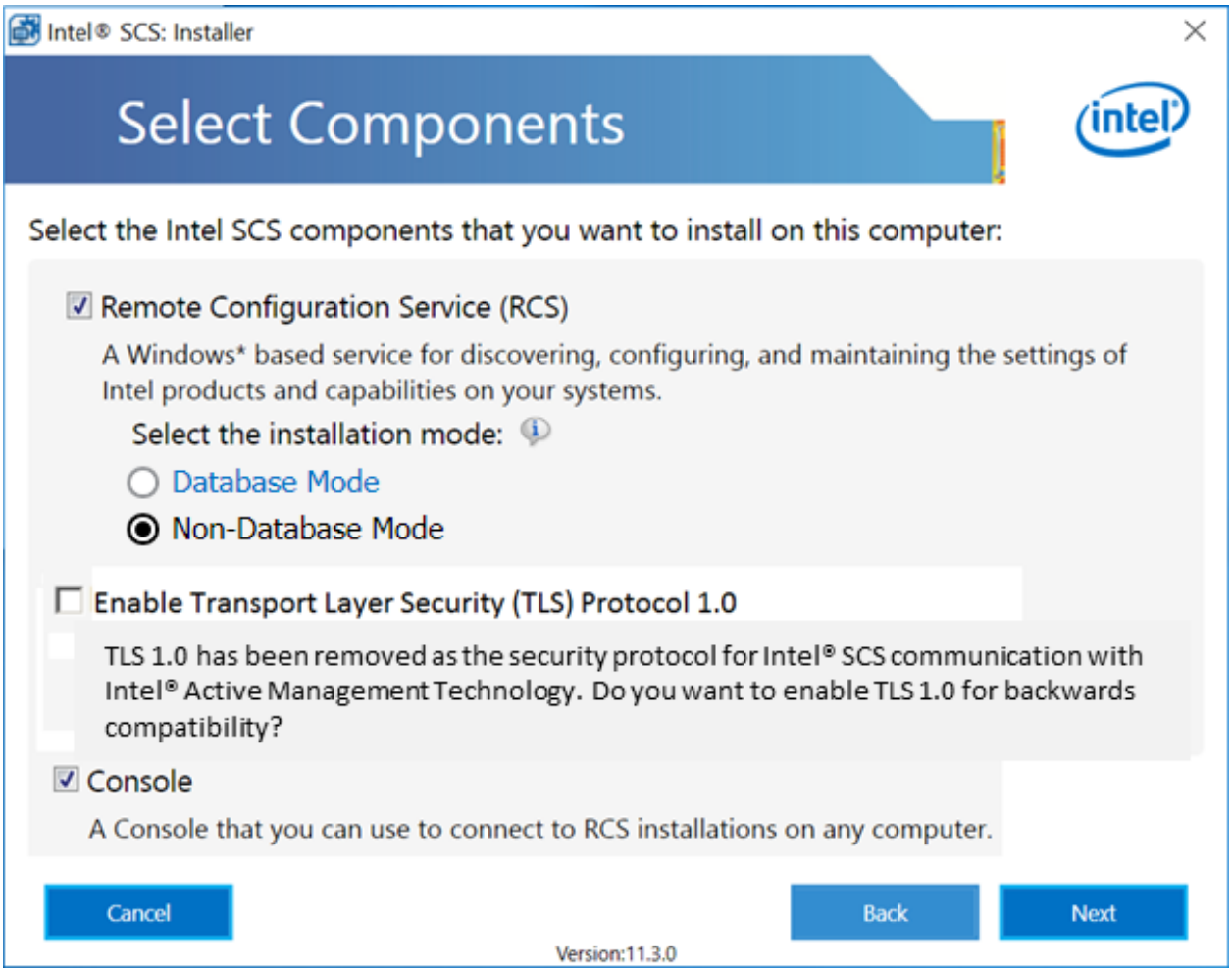


Figure 3-6: Select Components Window

4. Select the check boxes of the components that you want to install on this computer:
   - **Remote Configuration Service (RCS)** – Installs the RCS.

     Note:

     When installing the RCS, make sure that the **Non-Database Mode** option is selected.

   - **Enable TLS 1.0 Protocol for Encryption** – Enables the TLS 1.0 protocol for encryption. Intel SCS defaults to TLS 1.1 or TLS 1.2 (depending on your Intel AMT version) to encrypt communication to Intel AMT. TLS 1.0 has been deprecated as the security protocol for Intel SCS communication with Intel AMT, as the TLS 1.0 protocol has identified security vulnerabilities, including CVE-2011-3389 and CVE-2014-3566.

     Intel SCS allows users to enable TLS 1.0 protocol support for backwards compatibility with legacy Intel AMT platforms. For instructions on how to disable TLS 1.0 protocol support, see Configuring Transport Layer Security (TLS) Protocol Support on page 72.
   - **Console** – Installs the Console. You can install this component on any computer that can connect to the computer running the RCS.
5. Click **Next**. A confirmation dialog box appears. Select **Yes** to confirm that you want to enable TLS 1.0 Protocol support, or select **Cancel** to return to the Select Components window.
6. If you selected the option to install the RCS, the RCS User Account window opens. This window defines the user under which the RCS will run.

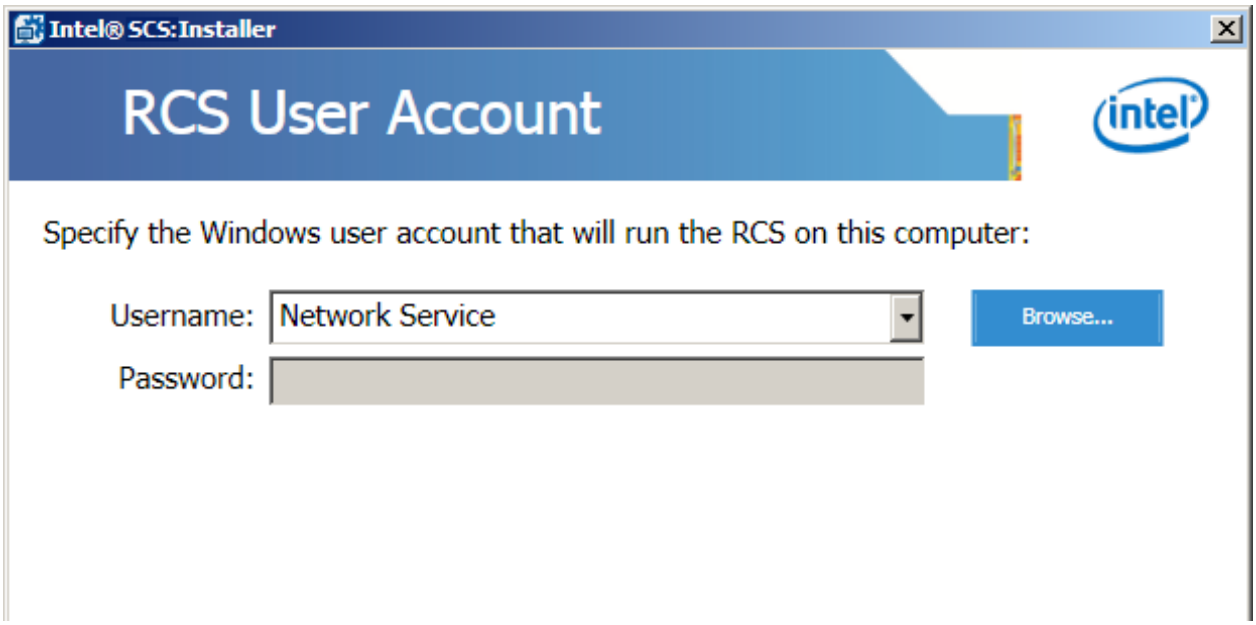


Figure 3-7: RCS User Account Window

Note:

In the Username field, by default, the Network Service account is selected. It is recommended to run the RCS using this built-in security account (see Using the Network Service Account on page 37).

7. (Optional) If you do not want to use the Network Service account:
   a. Click **Browse**. The Select Users or Groups window opens.
   b. Enter the user that will run the RCS on this computer. Enter the username in the format domain\username.
   c. Click **OK**. The Select Users or Groups window closes.
   d. In the Password field, enter the password of the user you selected (only the Network Service account does not require a password).
8. Click **Next**. The Storage Encryption Key window opens. This window installs the encryption key for the RCS to use when accessing the data files.

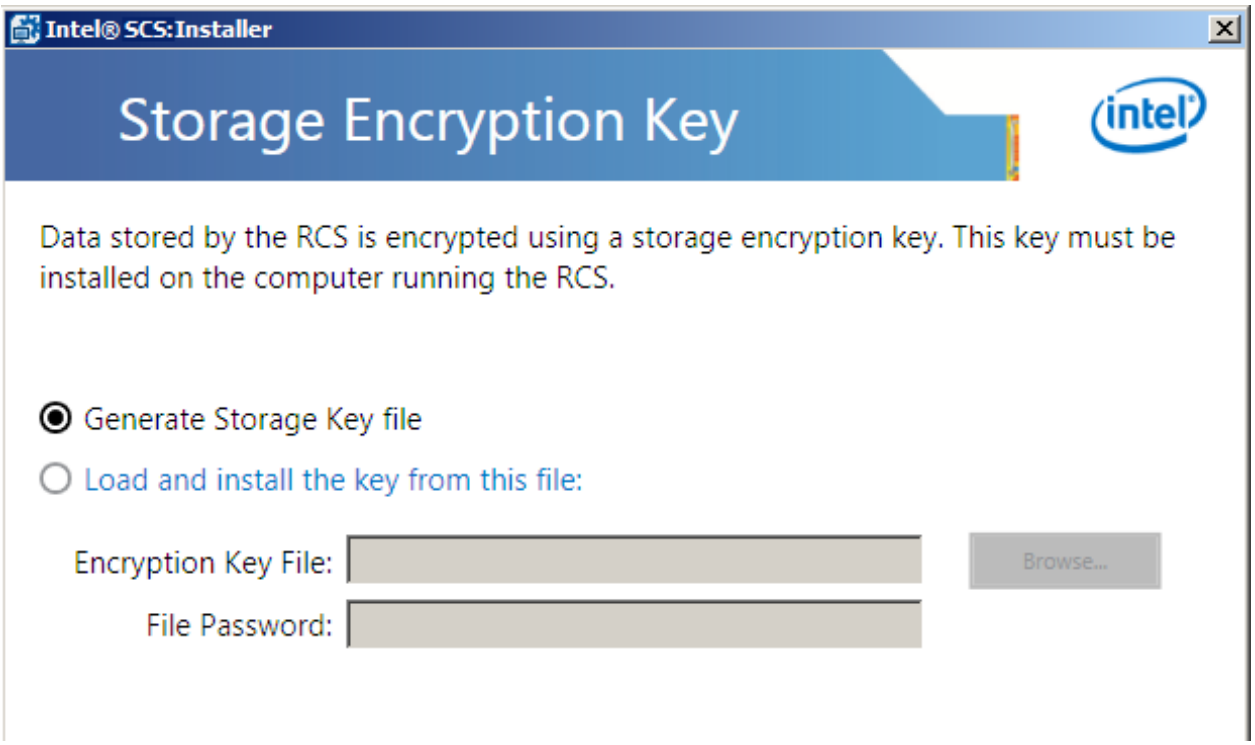


Figure 3-8: Storage Encryption Key Window

9. Select one of these:
   - **Generate storage key file** – Select this option to automatically create and install the storage encryption key.
   - **Load and install the key from this file** – You can select this option if you already have a storage encryption key (for example, you are moving the RCS to another computer). If you select this option, click **Browse** and select the storage encryption key file. In the File Password field you must also enter the password that was used to encrypt the key file.
10. Click **Next**. The Confirmation window opens. This window shows information about the selections you made.
11. (Optional) The default installation folder is `C:\Program Files (x86)\Intel\SCS12`.

    If you want to change this location, type a new path in the Install path field or click **Browse** to select it.

12. Click **Install**. The Installation Progress window opens. When installation is complete, a message is shown.
13. Click **Next**. The Completed Successfully window opens.
14. Click **Finish**. The Installer closes. The RCS is installed with default settings. If necessary, you can change these settings (see Defining the RCS Settings on page 77).
15. If you selected the **Generate storage key** option you must create a backup of the storage encryption key that the Installer created and installed automatically. You can export this encryption key to a file, as described in the procedure in Moving the RCS to a Different Computer on page 58

3.8 User Permissions Required to Access the RCS

Configuration methods that use the RCS require these users to have permissions to connect to the RCS:

- The user account running the Configurator
- All users that want to use the Console

If a user has administrator permissions on the computer running the RCS they will be able to connect to the RCS. Users with administrator permissions can use all the options available in the Console. If you do not want to give a user administrator permissions you can do these procedures instead:

- Defining DCOM Permissions below
- Defining WMI Permissions on the next page

3.8.1 Defining DCOM Permissions

This procedure describes how to define DCOM permissions.

To define DCOM permissions:

1. On the computer running the RCS open a command prompt window, enter `dcomcnfg` and press <Enter>. The Component Services window opens.
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 opens.
4. Click the **COM Security** tab. The COM Security tab opens.

   Figure 3-9: COM Security Tab

5. From the Access Permissions section:
   a. Click **Edit Limits**. The Access Permission window opens.
   b. Make sure that all users that need to connect to the RCS 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 Activation Permissions section:
   a. Click **Edit Limits**. The Launch Permission window opens.
   b. Make sure that all users that need to connect to the RCS appear in the list and have these 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. From the Console Root tree, select **Component Services** > **Computers** > **My Computer**> **DCOM Config** > **RCSServer**.

9. Right-click RCSServer and select Properties. The RCSServer Properties window opens.
10. Click the **Security** tab. The Security tab opens.
11. From the Configuration Permissions section:
    a. Select **Customize** and click **Edit**. The Change Configuration Permission window opens.
    b. Make sure that all users that need to connect to the RCS appear in the list and have the Full Control and Read permissions.
    c. Click **OK**. The Change Configuration Permission window closes.
    d. Click **OK**. RCSServer Properties window closes.
12. Close the Component Services window.

3.8.2 Defining WMI Permissions

Intel SCS includes four namespaces that control access to the RCS:

- `Intel_RCS` – Give permissions to this namespace to users who need to do operations on Intel AMT systems using the RCS. The user account running the Configurator needs permissions on this namespace.
- `Intel_RCS_Editor` – Give permissions to this namespace to users who need to connect to the RCS to define profiles or settings in the RCS. It is recommended to give permissions to this namespace only to users who are "administrators".
- `Intel_RCS_Master_Password` – Give permissions to this namespace to users who need to use the RCS to calculate or get the Digest Master Password.
- `Intel_RCS_Systems` – Give permissions to this namespace to users who need to use the monitoring options of the RCS (in database mode).

For each namespace, these are the necessary WMI permissions:

- Execute Methods
- Full Write
- Remote Enable

(These permissions are set in the Security tab of the WMI Control (Local) Properties window.)

Intel SCS includes a utility that you can use to give these permissions to the relevant user and group accounts. The RCS Utility (`RCSUtils.exe`) is located in the `Utils` folder.

Example #1: Adding a user named "MyUser" to the `Intel_RCS` namespace only:

```
RCSutils.exe /Permissions Add MyUser
```

Example #2: Adding a user to all the RCS namespaces:

```
RCSUtils.exe /Permissions Add MyUser /RCSNamespace All
```

Note:

You must run the RCS Utility on the computer where the RCS is installed and running. The local user account running the RCS Utility must have administrator permissions on the computer. On operating systems with User Account Control (UAC), the utility must be "Run as administrator". For more information, refer to the `Intel(R)_SCS_RCSUtility.pdf` also located in the `Utils` folder.

3.9 Backing up Data

The type of installation you selected causes the RCS to store data in files or in an SQL database. If one of the data files or database tables is damaged or missing, the RCS cannot operate correctly. Thus, it is important to make a regular backup. (If you need to restore data from a backup, make sure that you stop the RCS first. After the data is restored, restart the RCS.)

If you installed RCS in:

- **Database Mode** – Schedule a regular backup of the database in SQL Server.
- **Non-Database Mode** – Make regular backups of the data files and store them in a secure location. You can use any backup method or application that will let you recover the data files when necessary. In non-database mode, the data used by the RCS is kept in these encrypted files:
  - `Profile.xml` – The configuration profiles
  - `DMP.dat` – Digest Master Passwords. This file only exists if at some time the RCS was set to use the Digest Master Password option (see Security Settings Tab on page 80).

  The data files of non-database mode are stored in a folder named `RCSConfServer` in the user profile directory of the account running the RCS. The location of the folder depends on the RCS User Account type:
  - If you install with the Network Service Acount: Windows\ServiceProfiles\NetworkService\AppData\Local\Intel_Corporation
  - If you install the RC with a dedicated user account: Users\Username\AppData\Local\Intel_Corporation

3.9.1 Location of RCS Log Files

The log files of the RCS are located in a folder named `RCSConfServer` in one of these hidden locations:

- ProgramData\Intel_Corporation
- Documents and Settings\All Users\Application Data\Intel_Corporation

The log file is named `RCSLog.log` and records all operations and actions done by the RCS. Each time the log file becomes too large, or the RCS is restarted, the file content is moved to a new file with this format: `RCSLog.logYYYY-MM-DD-HH-MI-SS.log`.

3.10 Modifying an Existing Installation

This section describes how to modify an existing installation.

3.10.1 Removing/Adding Components

This procedure describes how remove or add components to an existing installation.

To add/remove components:

1. Double-click `IntelSCSInstaller.exe`.

   Note:

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

   The Welcome window opens.

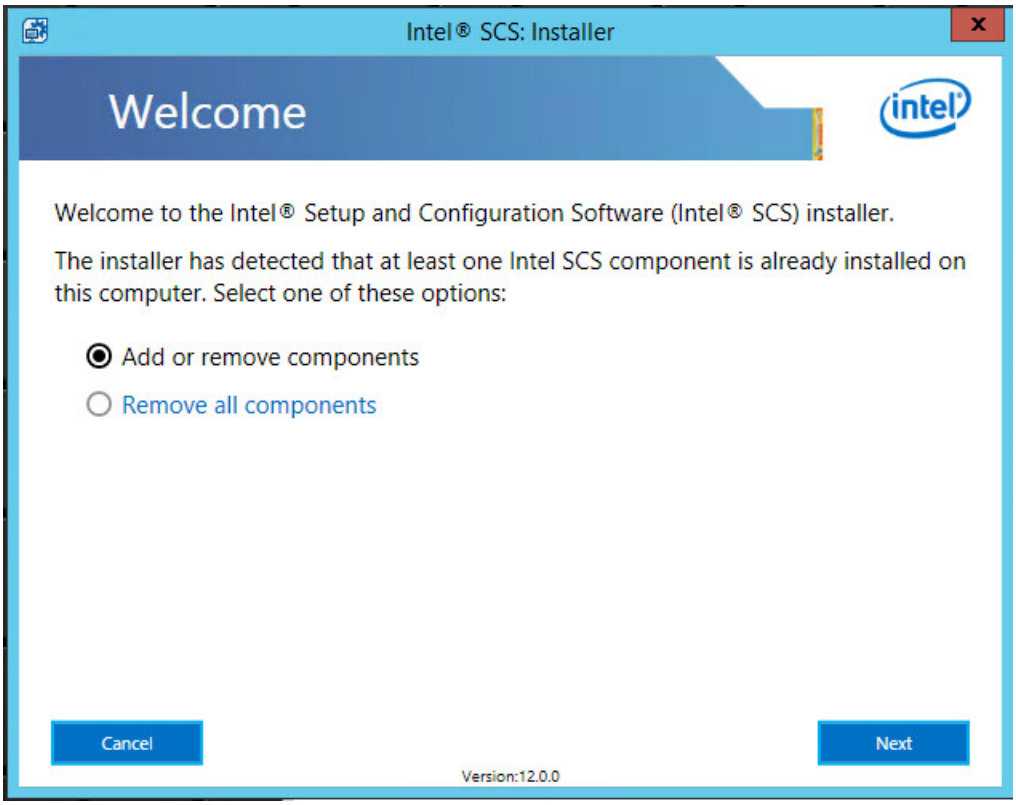


   Figure 3-10: Welcome Window

2. Select one of these:
   - **Add or remove components** – Lets you make changes to an existing installation. Continue to step 3.
   - **Remove all components** – Removes all Intel SCS components installed on this computer. Continue to step 5.

3. Click **Next**. The Modify Components window opens.

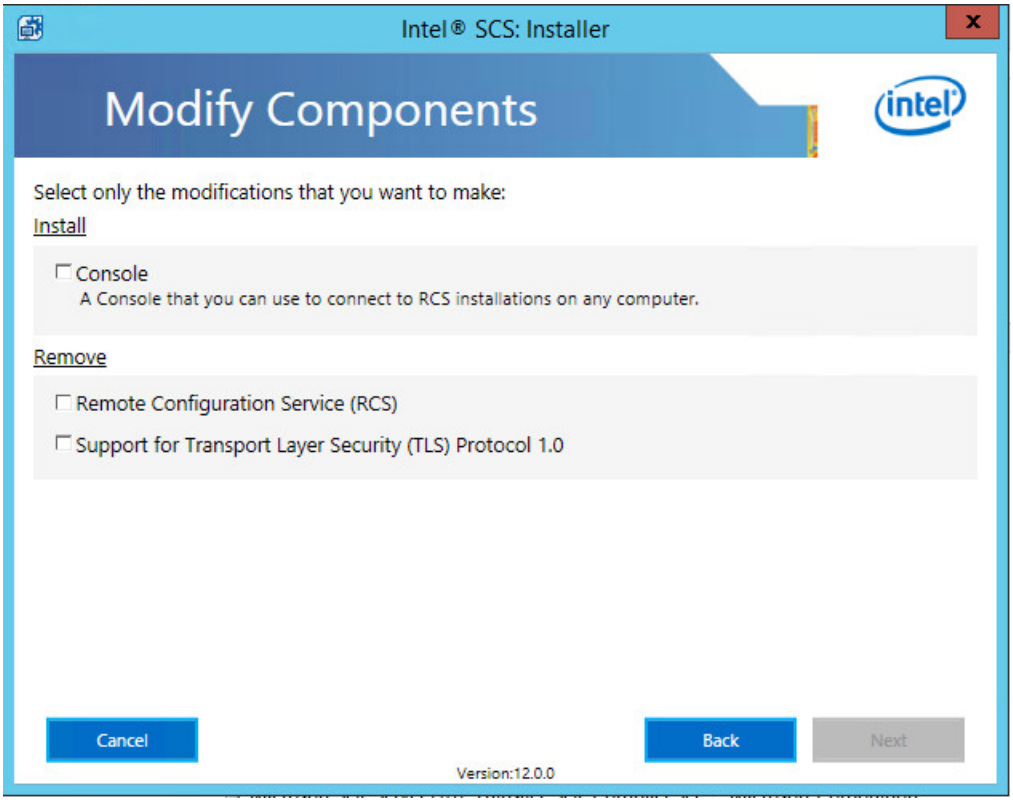


Figure 3-11: Modify Components Window

4. Select the modifications that you want to make:
   - In the Install section, select only the check boxes of the components that you want to install.
   - In the Remove section, select only the check boxes of the components that you want to uninstall.

5. Click **Next**. The Storage Key Extraction window opens. (This window is only shown if you are uninstalling the RCS.) This window lets you extract and save a copy of the encryption key that was used by the RCS to encrypt data. It is highly recommended to extract and save this key in a secure location.

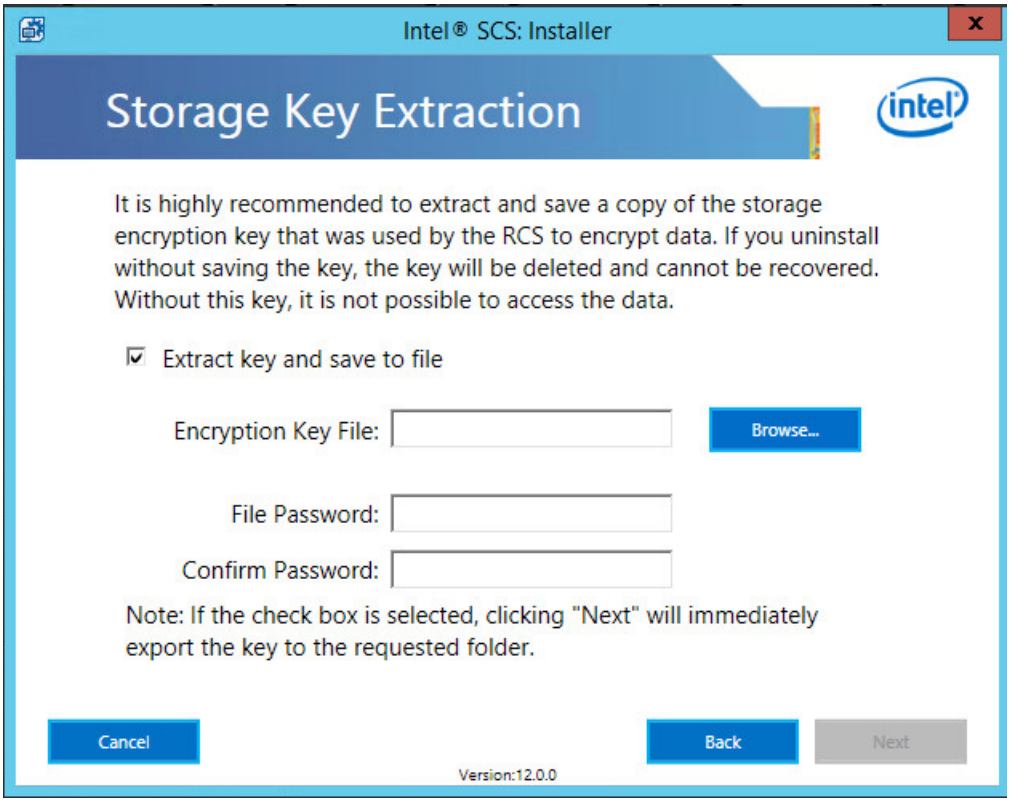


Figure 3-12: Storage Key Extraction Window

   a. In the Encryption Key File field, enter a name for the key file. It is recommended to save the file with a `.key` extension. By default, the file is created in the folder where the Installer is located. Alternatively you can click **Browse** to select a folder and filename.

   b. In the Password fields enter a password that will be used to encrypt the file. For the required format, see Password Format on page 11.

6. Click **Next** to continue to the Confirmation window. (If you selected to install the RCS, additional windows open. Supply the necessary data in each window.)
7. (Optional) By default, when uninstalling the RCS, the log files are not deleted. If you want to delete the log files, select the **Delete the RCS log files** check box. Selecting this check box will delete all files with a `.log` extension that exist in the root of the `RCSConfServer` folder. (Log files in any existing sub folders, created by the CA plugin for example, are not deleted.)
8. Click **Modify** (or **Remove** if you are only uninstalling). A window opens showing the progress of the changes that you selected. When complete, a message is shown.
9. Click **Next**. The Completed Successfully window opens.
10. Click **Finish**. The Installer closes.

Note:

If you have installed Intel SCS using the user interface provided by `IntelSCSInstaller.exe`, we recommend that you uninstall using the same method. If you have previously chosen to install using the `IntelSCSInstaller.exe` UI, and you wish to remove components using a silent installation, as described in Silent Installation on page 67, the onus is on you to remove the files `SCS12\IntelSCSInstaller.exe` and `SCS12\IntelSCSInstaller.exe.config`, and any remaining log files and folders associated with them.

3.10.2 Changing the Database

During installation of the RCS (in database mode), the RCS is configured to connect to a specific SQL database. After installation it is possible to reconfigure the RCS to connect to a different database. This is done using the Console.

To change the database connection of the RCS:

1. Make sure that you know the exact name of the replacement database and have the Storage Encryption Key file (and file password) for that database.
2. In the Console, select **Tools** > **Settings** > **Storage**. The Storage tab opens.
3. In the Storage Settings section, specify the database server name and the name of the replacement database. It is also possible to change the type of authentication that the RCS will use.
4. In the Storage Security section, click **Import**. The Open window opens.
5. Select the Storage Encryption Key file and click **Open**. The Enter Passphrase window opens.
6. Enter the password that was used to encrypt the key file and click **OK**.
7. Click **OK** and then **Yes** to confirm that you want to restart the RCS and apply the changes you have defined. The Settings window closes.
8. Select **Tools** > **Refresh**. The Console and the RCS are now connected to the replacement database.

3.10.3 Moving the RCS to a Different Computer

Some of the data used by the RCS is sensitive (for example, passwords). To protect this data, the RCS encrypts sensitive data before storing it in the SQL database (database mode) or data files (non-database mode). The data is encrypted using an encryption key. If you want to move the RCS to a different computer, you must supply the key when installing the RCS.

These are the required steps:

1. Make sure that you have the Storage Encryption Key file (and file password) for that database. If you do not have the key file, you can export it.
2. Install the RCS on the target computer. During installation, select the key file in the Storage Encryption Key window of the Installer.

To export the encryption key:

1. In the Console, select **Tools** > **Settings** > **Storage**. The Storage tab opens.
2. In the Storage Security section, click **Export**. The Save As window opens.
3. By default, the name of the exported key is `RCSStorage.key`. You can change this name if you want. Specify the location where you want to save the key file and click **Save**. The Enter Passphrase window opens.
4. Enter a password that will be used to encrypt the certificate file and click **OK**.
5. Click **OK** to close the Settings window. Make sure that you keep this key file and password in a secure location.

3.10.4 Deleting the Database

The Installer does not uninstall the database. If you are sure that you want to delete an Intel SCS database, and lose all data that it contains, you can use the `DeleteDB` command of the Database Tool.

This is the syntax and parameters for the `DeleteDB` command:

```
DatabaseTool.exe DeleteDB DBServer=<DB server> DBName=<DB name>
[Username=<SQL Login ID> Password=<SQL password>]
```

`DBServer=`	The name (FQDN) or IP address of the SQL Server
`DBName=`	The name of the database that you want to delete
`Username=`	By default, the credentials of the user account running the Database Tool are used to authenticate with SQL Server. If you want the Database Tool to use SQL Server authentication instead, use this parameter to supply the Login ID.
`Password=`	The password of the SQL Server account (only necessary if the user was supplied in the `Username=` parameter)

Examples

Example #1: Deleting a database on the local SQL Server:

```
DatabaseTool.exe DeleteDB DBServer=(local) DBName=TestDB
```

Example #2: Deleting a database on a remote SQL Server

```
DatabaseTool.exe DeleteDB DBServer=192.168.1.10 DBName=TestDB
```

Example #3: Deleting a database using SQL Server authentication:

```
DatabaseTool.exe DeleteDB DBServer=192.168.1.10 DBName=TestDB Username=MySQLUser
Password=P@ssw0rd
```

3.11 Upgrading Intel SCS

You can use the current version Intel SCS installer (`IntelSCSInstaller.exe`) to upgrade from these versions only:

- Intel SCS 10.x, 11.x, 12.x

The installation will be upgraded to the same mode (database/non-database). You cannot use the installer to change modes.

Upgrading Intel SCS to the current version means that you must upgrade all installed instances of the Console, RCS, and the Intel SCS data. In addition, you also need to replace the executable files of the other Intel SCS components that you use with the current version executables. (The Intel SCS 10.x and 11.x versions of the Configurator are compatible with current version Intel SCS components, but it is recommended to use the components included in the current Intel SCS version instead.)

If you are using the Intel SCS Add-on for SCCM, then you will need to upgrade that component to the latest version.

As of Intel SCS 12.2, the encryption algorithm for `SCSEncryption.exe` has been strengthened. If the XML file was encrypted using the discontinued algorithm, decrypt the file using `SCSEncryption.exe`, then re-encrypt it with `SCSEncryption.exe` to encrypt with the new supported algorithm.

3.11.1 Before Starting the Upgrade

In a production environment, the upgrade process requires some preparation and planning. This is because when upgrading the RCS and the Intel SCS data, you need to select a time when you can safely stop the RCS.

Before starting the upgrade process it is highly recommended to:

1. Plan for the upgrade by selecting a time when very few configuration requests will be sent to the RCS. In your software deployment mechanism, cancel or delay deployment packages that include maintenance or configuration requests that will be sent to the RCS.
2. In database mode, make sure that no jobs will be running during the upgrade.
3. When you are ready to start the upgrade, stop and disable the RCS. To do this, stop the Windows service named `RCSServer` and change the Startup Type to "Disabled". If you do not disable the RCS, any configuration requests that are received during the upgrade process might cause the upgrade to fail and even corrupt the existing data.
4. Make a full backup of the Intel SCS data:
   - In database mode, make a full backup in SQL Server
   - In non-database mode, refer to the User Guide of the version of Intel SCS that is currently installed

> **Note:**
>
> The upgrade process does not include a "rollback" process. If the upgrade fails and the data is corrupted the only way to recover is by restoring a full backup of the original data.

3.11.2 Upgrading Non-Database Mode

This procedure describes how to upgrade non-database mode of Intel SCS.

To upgrade non-database mode of Intel SCS:

1. Make sure that you have made a full backup and disabled the RCS (see Before Starting the Upgrade on the previous page).
2. Double-click `IntelSCSInstaller.exe`. The Welcome window opens.

   Note:

   This window shows the currently installed components that the installer will upgrade on this computer. If you want to add a component, run the installer again after upgrade is complete.

3. Click **Next**. The RCS User Account window opens.

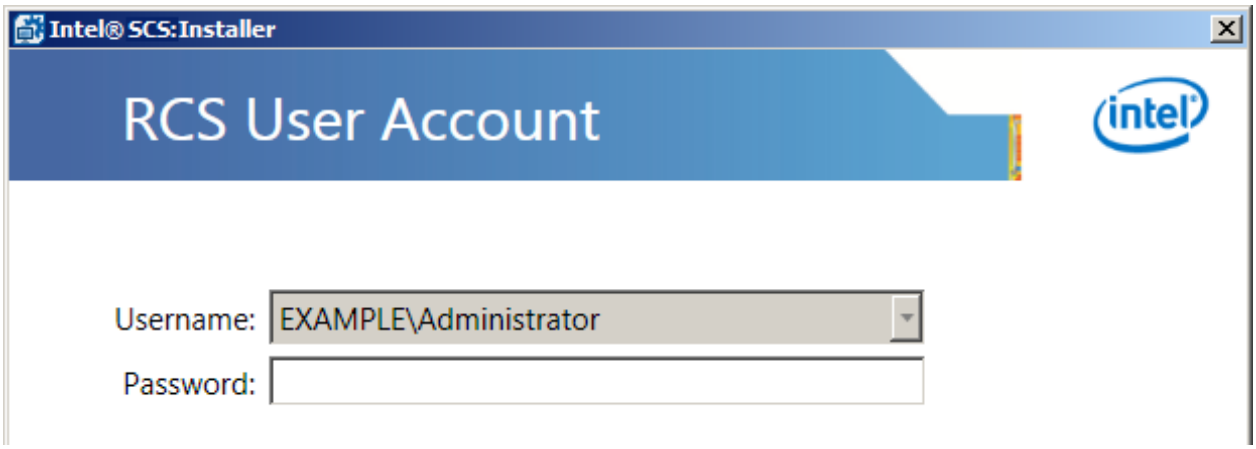


Figure 3-13: RCS User Account Window

4. Supply the password of the user account under which the RCS runs on this computer. (The Network Service account does not require a password.)

5. Click **Next**. If the Installer detects that the RCS has not been disabled, the Disable RCS window opens.

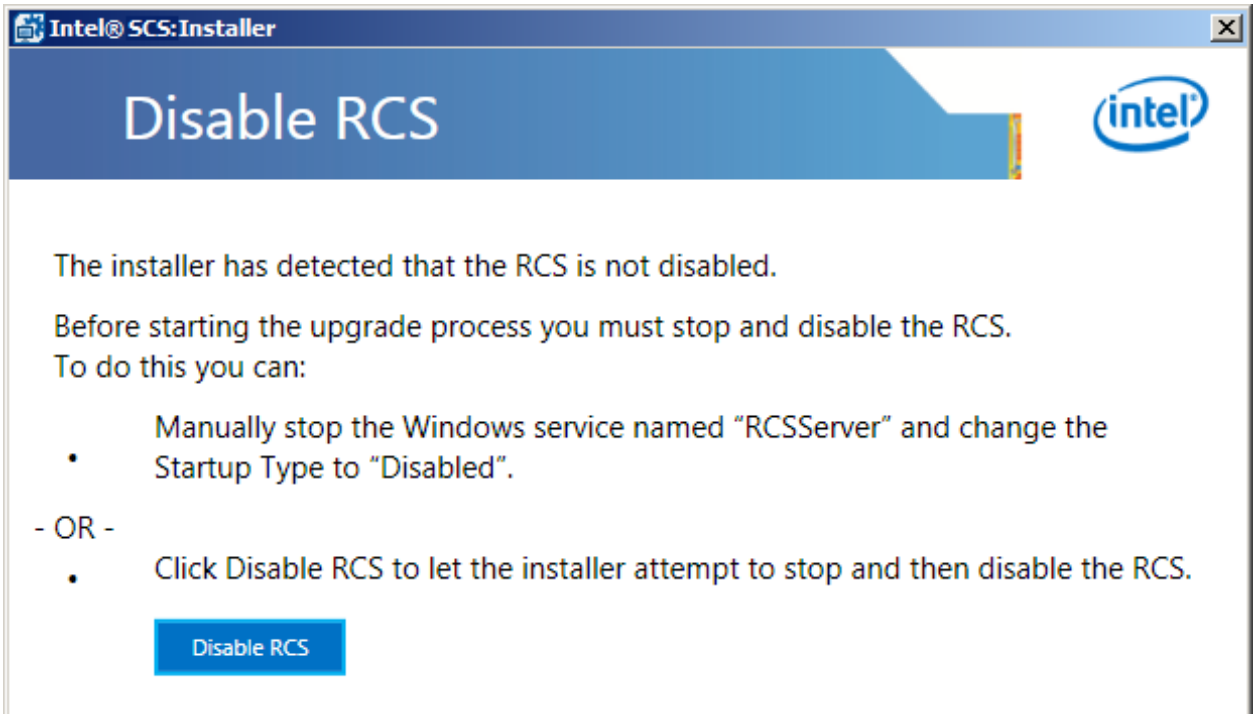


Figure 3-14: Disable RCS Window

If this window is shown, you can either:

- Manually stop the Windows service named "RCSServer" and change the Startup Type to "Disabled". (It is not necessary to close the Installer.)

-OR-

- Click **Disable RCS** to let the Installer attempt to stop and then disable the RCS.

When the Installer detects that the RCS is disabled a message is shown and the Next button is enabled.

6. Click **Next**. The Confirmation window opens. This window shows the location of the installation folder.

> **Note:**
>
> If the previous version was installed in the default location, the current version will be installed in the default location (`C:\Program Files (x86)\Intel\SCS12`). If not, the current version will be installed in the same folder in which you installed the previous version of Intel SCS.

7. Click **Upgrade**. The upgrade starts and the Upgrade Progress window opens. When the upgrade finishes the Next button is enabled.
8. Click **Next**. A window opens with information about the success or failure of the upgrade.
9. Click **Finish**. The Installer closes.

3.11.3 Upgrading Database Mode

This section describes how to upgrade database mode.

Note:

Before starting the upgrade process, see Before Starting the Upgrade on page 60.

3.11.3.1 Upgrading the Database

In many organizations, the company databases are managed by a database administrator (DBA). The DBA (or you) can use the Database Tool, located in the RCS folder, to upgrade the database. The Database Tool (`DatabaseTool.exe`) is a simple CLI that you can use locally on the SQL Server or remotely.

This is the syntax and parameters for the `UpgradeDB` command:

```
DatabaseTool.exe UpgradeDB /RCSisDisabled DBServer=<DB server>
DBName=<DB name> [Username=<SQL Login ID> Password=<SQL password>]
[KeyFileName=<filename>]
```

`/RCSisDisabled`	This parameter is mandatory and exists to remind you that you must disable the RCS before using the `UpgradeDB` command
`DBServer=`	The name (FQDN) or IP address of the SQL Server
`DBName=`	The name of the database
`Username=`	By default, the credentials of the user account running the Database Tool are used to authenticate with SQL Server. If you want the Database Tool to use SQL Server authentication instead, use this parameter to supply the Login ID.
`Password=`	The password of the SQL Server account (only necessary if the user was supplied in the Username parameter)
`KeyFileName=`	This parameter is relevant only during upgrade of version 8.x databases. By default, the Database Tool creates an encryption key file named `RCSStorage.key` in the folder where the Database Tool is located. You can use this parameter to supply an alternative path and filename.

Examples

Example #1: Upgrading a database on the local SQL Server:

```
DatabaseTool.exe UpgradeDB DBServer=(local) DBName=TestDB
```

Example #2: Upgrading a database on a remote SQL Server:

```
DatabaseTool.exe UpgradeDB DBServer=192.168.1.10 DBName=TestDB
```

Example #3: Upgrading a database using SQL Server authentication:

```
DatabaseTool.exe UpgradeDB DBServer=192.168.1.10 DBName=TestDB Username=MySQLUser
Password=P@ssw0rd
```

3.11.3.2 Upgrading the RCS and Console

This procedure describes how to upgrade database mode of Intel SCS.

To upgrade database mode of Intel SCS:

1. Make sure that you have made a full backup and disabled the RCS (see Before Starting the Upgrade on page 60).
2. Double-click `IntelSCSInstaller.exe`. The Welcome window opens.

> **Note:**
>
> This window shows the currently installed components that the installer will upgrade on this computer. If you want to add a component, run the installer again after upgrade is complete.

3. Click **Next**. The RCS User Account window opens.

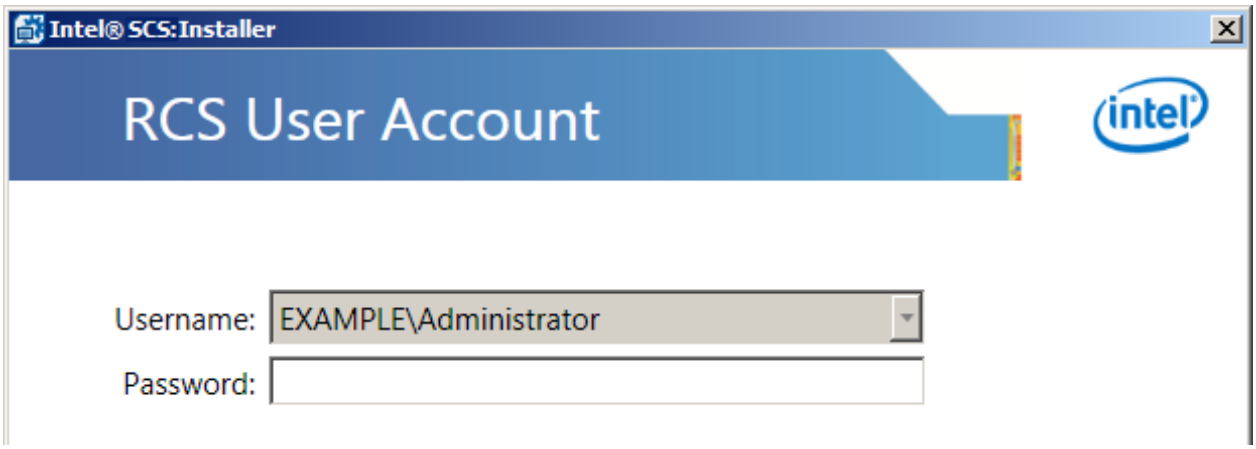


Figure 3-15: RCS User Account Window

4. Supply the password of the user account under which the RCS runs on this computer. (The Network Service account does not require a password.)

5. Click **Next**. If the Installer detects that the RCS has not been stopped and disabled, the Disable RCS window opens.

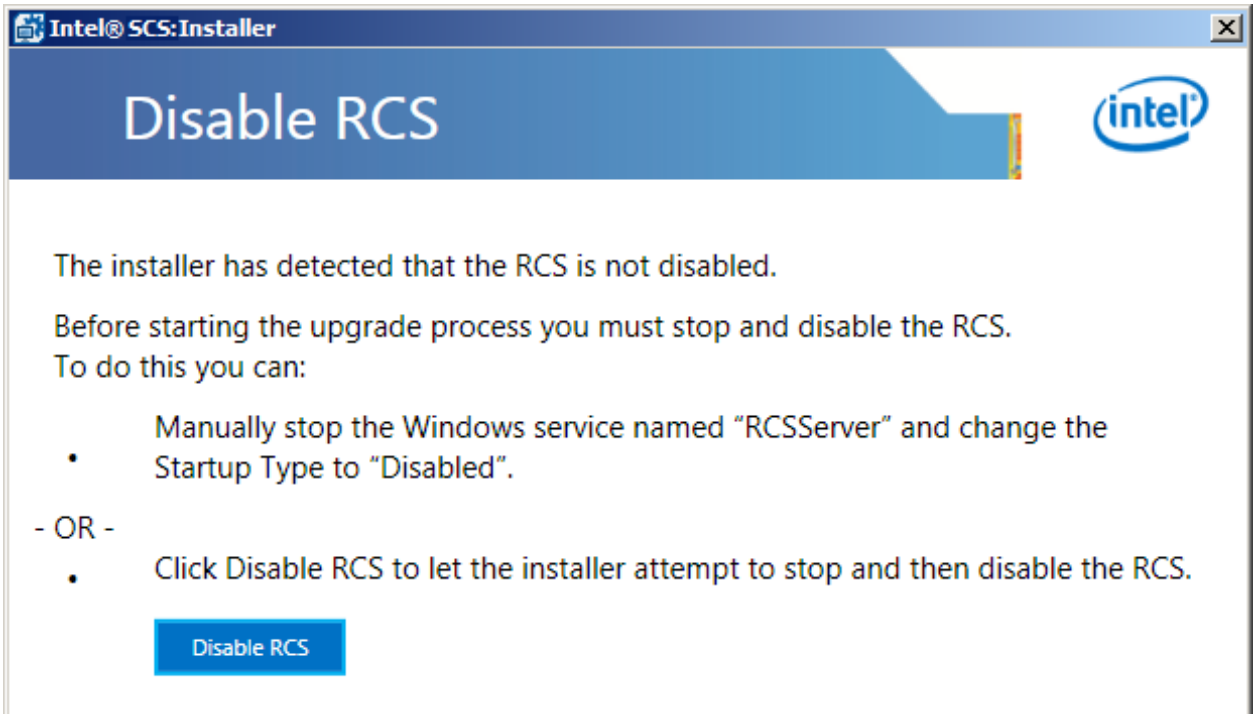


Figure 3-16: Disable RCS Window

If this window is shown, you can either:

- Manually stop the Windows service named "RCSServer" and change the Startup Type to "Disabled". (It is not necessary to close the Installer.)

-OR-

- Click **Disable RCS** to let the Installer attempt to stop and then disable the RCS.

When the Installer detects that the RCS is disabled a message is shown and the Next button is enabled.

6. Click **Next**. The Database Settings window opens. This window shows information about the location of the database and how the RCS authenticates with the database.

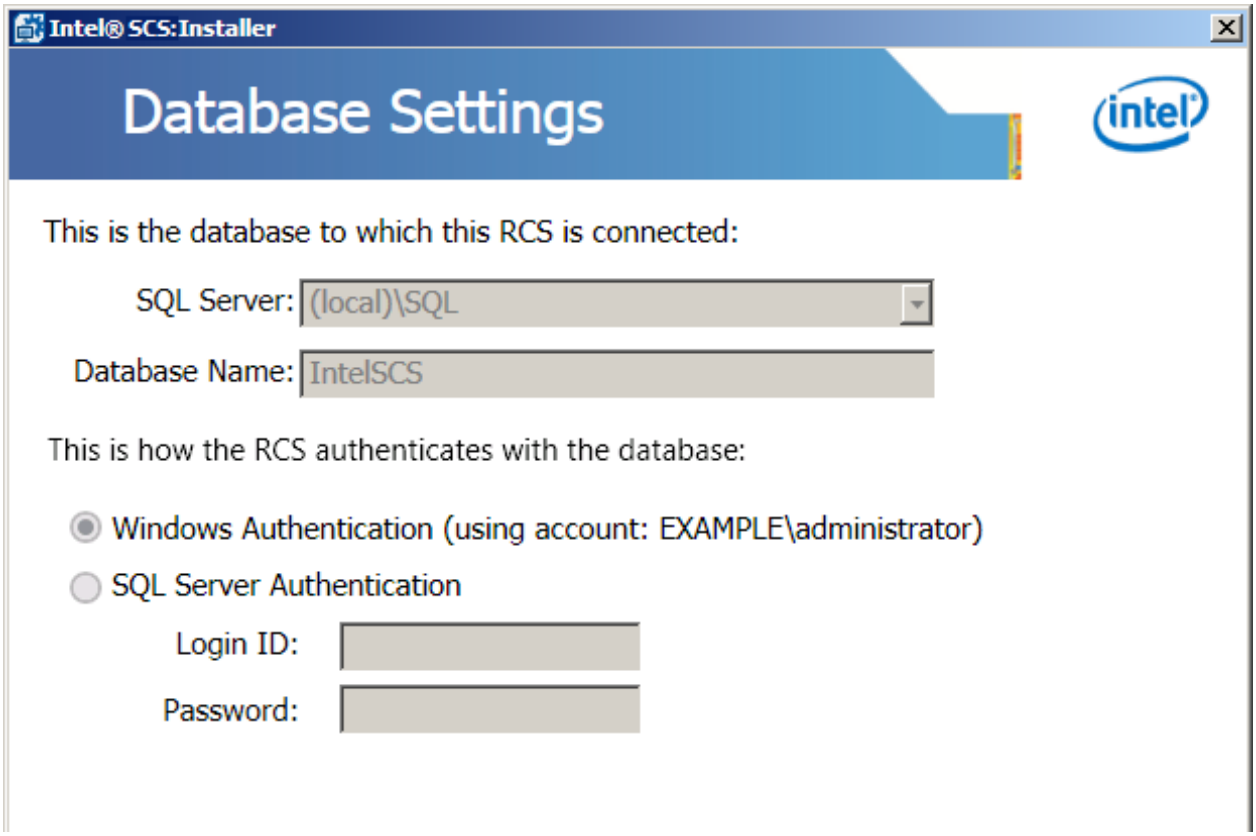


Figure 3-17: Database Settings Window

> **Note:**
>
> If the RCS is using SQL Server Authentication, you must supply the password of the SQL Server account that is shown in the Login ID field.

7. Click **Next**. The Installer connects to the database and checks the database version:
   - If you have not upgraded the database, continue from step 8.
   - If you have already upgraded the database, continue from step 9.
8. If the database has not already been upgraded, the Upgrade Intel SCS Database window opens. If you want the Installer to do the upgrade now:
   a. Click **Upgrade Database** and wait for the database upgrade to complete.
   b. When complete, click **Close**.

9. Click **Next**. The Confirmation window opens. This window shows the location of the installation folder.

> **Note:**
>
> If the previous version was installed in the default location, the current version will be installed in the default location (`C:\Program Files (x86)\Intel\SCS12`). If not, the current version will be installed in the same folder in which you installed the previous version of Intel SCS.

10. Click **Upgrade**. The upgrade starts and the Upgrade Progress window opens. When the upgrade finishes the Next button is enabled.
11. Click **Next**. A window opens with information about the success or failure of the upgrade.
12. Click **Finish**. The Installer closes.

3.12 Silent Installation

Intel SCS includes an additional installation file (`IntelSCSInstaller.msi`). This file is based on the Windows Installer CLI and uses the commands available in the standard installation mode. You can use this file to silently install/upgrade the RCS and the Console using a script.

> **Notes:**
>
> - The Windows Installer CLI is case-sensitive.
> - Running silent installation from a command line prompt might fail if one of the passwords contains certain characters (for example, a pipe | character). You can avoid these problems by always running silent installation commands in a batch file.
> - Before you can install the RCS in database mode, a database must first be created, and the user running RCS added to it using the Database Tool's `adduser` command. See Adding the RCS User to the Database on page 70 for more information.

The following table describes the options available.

Silent Install Options

Command/Property	Description
`/qn`	Install silently
`/l*v <filename>`	Create a verbose log file where `<filename>` is the name of the log file

Command/Property	Description
ADDLOCAL=	Install the components. Valid values: • **All** – Installs the RCS, Console, and TlsOptIn components. (TlsOptIn is not enabled by default; see Enabling TLS 1.0 Opt-in on page 70.) • **Service** – Installs RCS only. • **Console** – Installs Console only. • **TlsOptIn** – Installs the TLS 1.0 protocol for encryption between Intel SCS and Intel AMT (not enabled by default). See Enabling TLS 1.0 Opt-in on page 70.
REMOVE=	Uninstall the components. Valid values: • **All** – Installs the RCS, Console, and TlsOptIn components. • **Service** – Uninstalls RCS only. • **Console** – Uninstalls Console only. • **TlsOptIn** – Uninstalls the TLS 1.0 protocol for encryption between Intel SCS and Intel AMT.
To enable the TLS 1.0 opt-in, you must define this property:	
TLS10_OPT_IN_VAL=	The TLS 1.0 protocol opt-in setting (see Enabling TLS 1.0 Opt-in on page 70). Valid values: • **1** – Enable TLS 1.0 opt-in • **0** – Disable TLS 1.0 opt-in (default behavior)
If installing/upgrading the RCS, you must define these properties:	
LOGON_USERNAME=	The user under which the RCS will run, in the format Domain\Username. If you want to use the Network Service account, supply only the username: NetworkService. **Note:** If upgrading, you must supply the credentials of the user account under which the current version of the RCS is running.
LOGON_PASSWORD=	The password of the RCS user. Do not supply this property if you are using the Network Service account.
DB_MODE=	The database mode. Valid values: • **0** – Non-database mode • **1** – Database mode **Note:** If upgrading, do not supply this property.
If installing the RCS in database mode, you must also define these properties:	
SQL_SERVER=	The name of the SQL Server where the Intel SCS database is installed
DB_NAME=	The name of the Intel SCS database exactly as it is defined in the SQL Server

<table>
<tr><th>Command/Property</th><th>Description</th></tr>
<tr><td colspan="2">By default, the RCS is configured to use Windows authentication to connect to the database. If you prefer to use SQL Server authentication, define these properties:</td></tr>
<tr><td>SERVICE_SQL_USER=</td><td>The Login ID on the SQL Server</td></tr>
<tr><td>SERVICE_SQL_PASSWORD=</td><td>The password on the SQL Server</td></tr>
<tr><td colspan="2">These are additional (optional) parameters you can use when installing (not upgrading):</td></tr>
<tr><td>INSTALLDIR=</td><td>The default installation folder is: C:\Program Files (x86)\Intel\SCS12. If you want to change this location, use this property and supply the full path to the installation folder.</td></tr>
<tr><td>WMI_ADMIN_ACCOUNT=</td><td rowspan="2">You can use these properties to give WMI permissions on the RCS namespaces to the user accounts (or groups) that you specify. Each property gives permissions on different namespaces:
WMI_ADMIN_ACCOUNT – Gives permissions to all the namespaces that control access to the RCS (see Defining WMI Permissions on page 53). It is recommended to use this property only for user accounts who are “administrators”.
WMI_ACCESS_ACCOUNT – Gives permissions only to the Intel_RCS namespace.
You can specify the accounts by supplying the Security Identifier (SID) or the username, in this format: domain\username. To specify multiple user accounts, separate each user account with a semi-colon (;).
Examples:
WMI_ACCESS_ACCOUNT=example\myuser1;example\myuser2
WMI_ADMIN_ACCOUNT=S-1-5-21-725345543-602162358-527237240-205384;example\myuser2
Note:
In addition to WMI permissions, the user accounts will also automatically be given the DCOM permissions necessary to connect to the RCS. If the user accounts did not have any DCOM permissions on the computer running the RCS, you will need to restart the computer. (This is because of a Microsoft limitation the first time that a user account is granted DCOM permissions on a computer.)
When using these properties, any existing default or specific WMI permissions of users/groups on these namespaces are replaced.</td></tr>
<tr><td>WMI_ACCESS_ACCOUNT=</td></tr>
</table>

Adding the RCS User to the Database

If you plan to install the RCS in database mode, you must first have a working database created, and then add the user running RCS to it, using the Database Tool's `adduser`command. To do this, follow these steps:

1. Create, or have your DBA create, a database to use for installing in database mode. SeeCreating the Database on page 40 for instructions.
2. After creating the database in step 1, use the `adduser`command to give the RCS user access to the database. (See Adding the RCS User to the Database above for details.) If the RCS is to be run by the "Network Service" account, grant the local computer$ account access to the database. (See Using the Network Service Account on page 37 for more information.)

About the Storage Key File

When using the silent install option to install the RCS, you must supply the storage key file in the `STORAGE_KEY_FILE=` property. This file is created using the Database Tool (`DatabaseTool.exe`), located in the `RCS` folder. The command that you need to use depends on the type of installation:

- **Database mode** – The file is created when you create the database using the `CreateDB` command (see Creating the Database on page 40).
- **Non-database mode** – Use the `CreateStorageKey` command. For more information, refer to the CLI help of the Database Tool.

In database mode, the key is created when you upgrade the database (see Upgrading the Database on page 63). In non-database mode, use the `CreateStorageKey` command.

Note:

During upgrade of the RCS from version 10.x, 11.x, or 12.x, the existing storage key file will be used (it is not necessary to create or supply a new storage key file).

Enabling TLS 1.0 Opt-in

To ensure that TLS 1.0 protocol is enabled during silent installation, as part of the `IntelSCSInstaller.msi` command, you must

- Install the TLS 1.0 protocol by specifying `ADDLOCAL=All` or `ADDLOCAL=TlsOptIn`
- Set the corresponding registry value to enable TLS 1.0 by specifying `TLS10_OPT_IN_VAL=1`

The full command should appear as shown in Example #7: Installing RCS and TLS opt-in in database mode and enabling TLS 1.0 on the next page.

Note: TLS 1.0 has been deprecated as the security protocol for Intel SCS communication with Intel AMT. The TLS 1.0 protocol has identified security vulnerabilities, including CVE-2011-3389 and CVE-2014-3566. Intel SCS will default to TLS 1.1 or TLS 1.2 (depending on your Intel AMT version) to encrypt communication between Intel SCS software components and Intel AMT. Users can enable TLS 1.0 protocol support for backwards compatibility, both during installation of the Remote Configuration Server (RCS) and after installation/upgrade of the RCS.

Examples

Example #1: Installing database mode using Windows authentication

```
IntelSCSInstaller.msi /qn /l*v log.txt ADDLOCAL=All
LOGON_USERNAME=Example\RCSUser LOGON_PASSWORD="P@ssw0rd" DB_MODE=1
STORAGE_KEY_FILE="RCSStorage.key" STORAGE_KEY_FILE_PASSWORD="FileP@ssw0rd"
SQL_SERVER=sq1server.example.com DB_NAME=IntelSCS
```

Example #2: Installing database mode using SQL Server authentication

```
IntelSCSInstaller.msi /qn /l*v log.txt ADDLOCAL=All
LOGON_USERNAME=Example\RCSUser LOGON_PASSWORD="P@ssw0rd" DB_MODE=1
STORAGE_KEY_FILE="RCSStorage.key" STORAGE_KEY_FILE_PASSWORD="FileP@ssw0rd"
SQL_SERVER=sq1server.example.com DB_NAME=IntelSCS SERVICE_SQL_USER=sa
SERVICE_SQL_PASSWORD="MySQLP@ssw0rd"
```

Example #3: Uninstalling the RCS and the Console

```
IntelSCSInstaller.msi /qn /l*v log.txt REMOVE=All
```

Example #4: Installing non-database mode

```
IntelSCSInstaller.msi /qn /l*v log.txt ADDLOCAL=All
LOGON_USERNAME=Example\RCSUser LOGON_PASSWORD="P@ssw0rd" DB_MODE=0
STORAGE_KEY_FILE="RCSStorage.key" STORAGE_KEY_FILE_PASSWORD="FileP@ssw0rd"
```

Example #5: Upgrading version 11.x using Windows authentication

```
IntelSCSInstaller.msi /qn /l*v log.txt
LOGON_USERNAME=Example\RCSUser LOGON_PASSWORD="P@ssw0rd"
```

Example #6: Upgrading version 11.x using SQL Server authentication

```
IntelSCSInstaller.msi /qn /l*v log.txt
LOGON_USERNAME=Example\RCSUser LOGON_PASSWORD="P@ssw0rd"
SERVICE_SQL_USER=sa SERVICE_SQL_PASSWORD="MySQLP@ssw0rd"
```

Example #7: Installing RCS and TLS opt-in in database mode and enabling TLS 1.0

```
IntelSCSInstaller.msi /qn /l*v log.txt ADDLOCAL=”Service,TlsOptIn”
LOGON_USERNAME=vprodemo\itproadmin LOGON_PASSWORD="P@ssw0rd" DB_MODE=1
STORAGE_KEY_FILE="RCSStorage.key" STORAGE_KEY_FILE_PASSWORD="FileP@ssw0rd"
SQL_SERVER=sq1server.example.com DB_NAME=IntelSCS TLS10_OPT_IN_VAL=1
```

Example #8: Installing database mode and setting TLS 1.0 opt-in to false

```
IntelSCSInstaller.msi /qn /l*v log.txt ADDLOCAL=All
LOGON_USERNAME=vprodemo\itproadmin LOGON_PASSWORD="P@ssw0rd" DB_MODE=1
STORAGE_KEY_FILE="RCSStorage.key" STORAGE_KEY_FILE_PASSWORD="FileP@ssw0rd"
SQL_SERVER=sq1server.example.com DB_NAME=IntelSCS TLS10_OPT_IN_VAL=0
```

3.13 Configuring Transport Layer Security (TLS) Protocol Support

Intel SCS has deprecated the TLS 1.0 security protocol for Intel® SCS communication with Intel® AMT. The TLS 1.0 protocol has identified security vulnerabilities, including CVE-2011-3389 and CVE-2014-3566. Users can enable TLS 1.0 protocol support for backwards compatibility, both during installation/upgrade of the Remote Configuration Server (RCS) and after installation of the RCS.

In the registry of the computer running the RCS, the installer creates a DWORD key with the name "EnableTLS1.0":

- 32-bit operating systems: HKLM\SOFTWARE\Intel\Intel(R) Setup and Configuration Software\<*version*>\RCS\GeneralSettings
- 64-bit operating systems: HKLM\SOFTWARE\Wow6432Node\Intel\Intel(R) Setup and Configuration Software\<*version*>\RCS\GeneralSettings

When the RCS starts, it checks the value of this key.

If the key value is equal to 0, the RCS will default to TLS 1.1 or TLS 1.2 (depending on your Intel AMT version) protocol for encrypting network.

If the key value is equal to 1, the RCS will support both TLS 1.1/1.2 and TLS 1.0 protocols for encryption.

Chapter 4

Using the Console

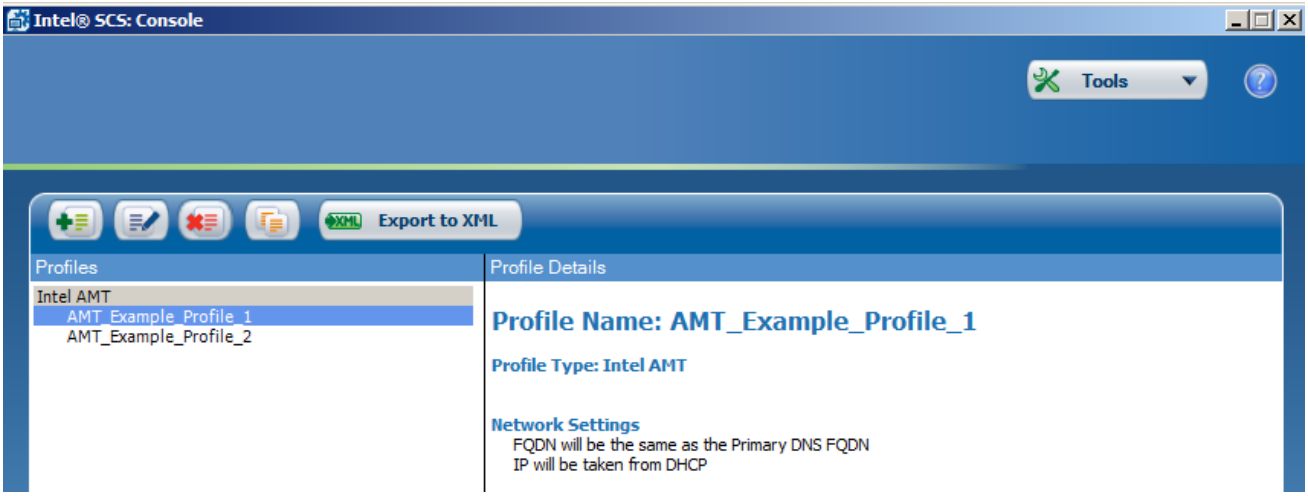
This chapter describes how to use the Console.

For more information, see:

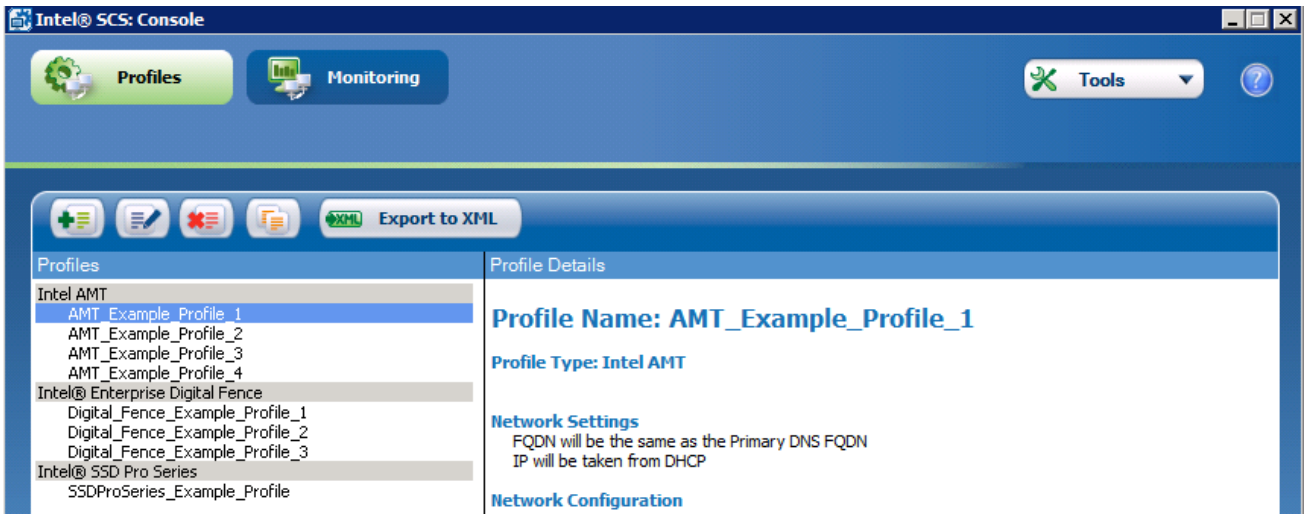
4.1 About the Console

The Console is the user interface to the RCS. The Console can be installed on the same computer as the RCS, or any other computer that can connect to the RCS. When the Console connects to the RCS, the database mode of the RCS defines which options are available from the Console.

Non-Database Mode:



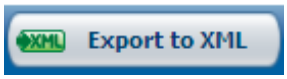
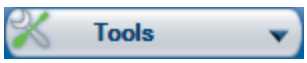
Database Mode:



Note:

Each window of the Console includes context sensitive help that shows when you press F1 or click the help icon.

Table 4-1: This table describes the options available from the Console.

Click	To do this...
	To work with profiles when in database mode. When selected, this button has a green background.
	Create a new profile (see Creating Configuration Profiles on page 82).
	Duplicate the profile selected in the left pane.
	Delete the profiles selected in the left pane. **Note:** Make sure that you do not delete a profile that is currently being used. (See About Deleting and Modifying Profiles on page 87.)
	Export the profiles to a CSV file. See Exporting Profiles to CSV.
	Edit the profile selected in the left pane.
	Export a profile to an XML file to use with unified configuration. For more information, see: • Exporting Profiles from the Console on page 83 • Unified Configuration Process on page 9
	Use the monitoring options available in database mode. When selected, this button has a green background. For more information, see: • Monitoring Systems on page 159 • Managing Jobs and Operations on page 181
	When monitoring in database mode, open the systems in the current view in the the Intel® Manageability Commander Tool. See Viewing Systems Using the Intel® Manageability Commander Tool on page 169.
	For information about the options included in the Tools menu, see: • Connecting to the RCS on the next page • Defining the RCS Settings on page 77 • Importing PSK Keys from a File on page 85 • Defining Manual Configuration (Multiple Systems)

4.2 Connecting to the RCS

If you install the Console on a computer where RCS is running, the Console is automatically set to connect to the RCS on that computer. You can also install the Console on other computers in the network and then select to which RCS to connect.

You can change this setting at any time for each Console you install.

To define the service location for the Console:

1. In the Console, select **Tools** > **Connect to a different RCS**. The Connect to RCS window opens.

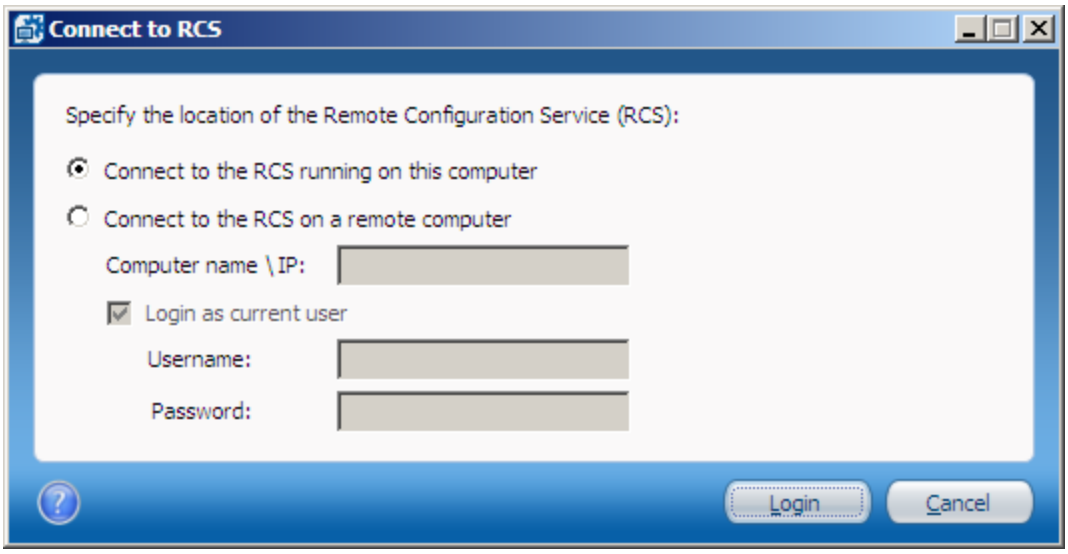


Figure 4-1: Connect to RCS Window

2. Select one of these:
   - **Connect to the RCS running on this compute**r – If the RCS to which you want to connect is installed on this computer, make sure that it is running and then select this option. The next time you start the Console on this computer the Console will automatically connect to the RCS.
   - **Connect to the RCS on a remote compute**r – Select this option if the RCS runs on a different computer in the network. Enter the name of the computer running the RCS (or the IP address). The Console will login using the current user credentials. Optionally, you can clear the **Login as current user** check box and enter credentials of a different user.
3. Click **Login**. When connection is established, the Connect to RCS window closes and the Console opens.

4.3 Defining the RCS Settings

The RCS is installed with default settings. If necessary, you can change these settings.

> **Note:**
>
> Before you can change the RCS settings, the Console must be connected to the RCS (see Connecting to the RCS on the previous page).

To change the default RCS settings:

1. In the Console, select **Tools** > **Settings**. The Configuration Options tab of the Settings window opens.

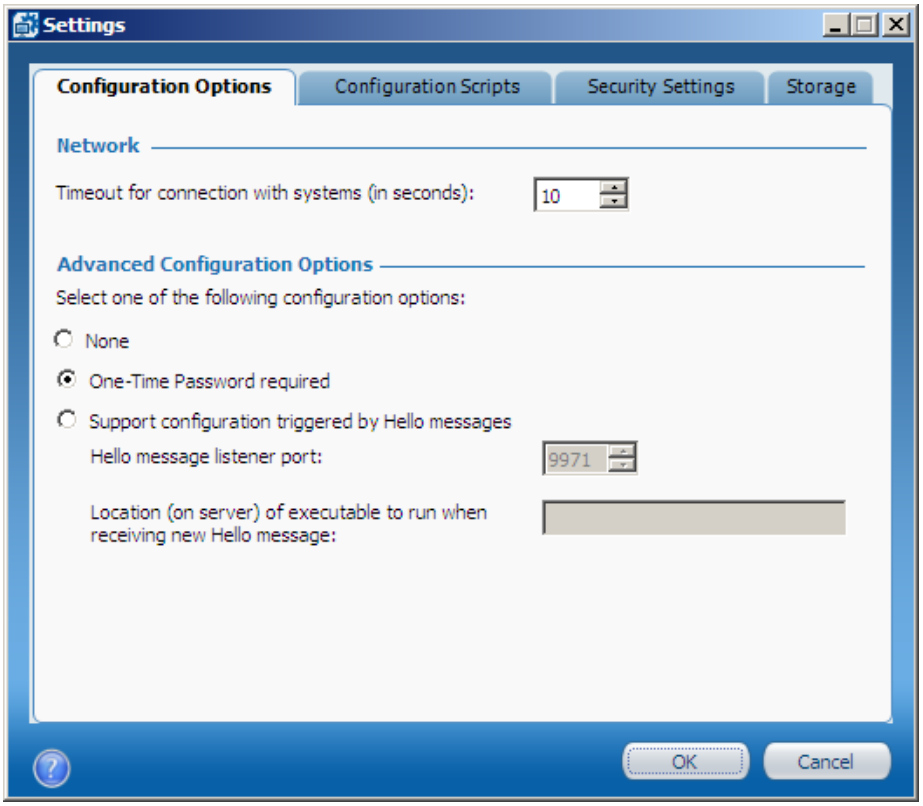


Figure 4-2: Configuration Options Tab

2. Define the settings that you want for this RCS and click **OK**. The settings are saved and the Settings window closes. For information about these settings, see:
   - Network on the next page
   - Advanced Configuration Options on the next page
   - Configuration Scripts Tab on page 79
   - Security Settings Tab on page 80
   - Storage Tab on page 81

Network

The RCS communicates with the Intel AMT device using the Transmission Control Protocol (TCP). During communication, if the device does not answer within a specified time the RCS cancels the communication. This default "Timeout" setting is 10 seconds. This is usually enough time for the device to respond. To change this default, enter a new value (between 10 and 80 seconds) in this field: Timeout for connection with systems (in seconds).

Note:

A large Timeout value can cause configuration/maintenance tasks done by the RCS to take longer than usual.

Advanced Configuration Options

Select which of the advanced configuration options you want to use:

- **None** – Select this option if you do not want to use any of the advanced configuration options described in this section.
- **One-Time Password required** – This option is only used during Remote Configuration (using PKI) For more information, see About Remote Configuration on page 209.
- **Support Configuration triggered by Hello messages** – Select this option only if you want the RCS to configure systems remotely using a script that you supply. For more information, see Remote Configuration Using Scripts on page 216. If you select this option:

  1. Specify the TCP port that the RCS will use to listen for Hello messages from the Intel AMT systems. The minimum value for the port is 1025. The default port is 9971.

  2. Specify the path to a script that will provide the required information about the Intel AMT systems. The script must be located on the computer running the RCS.

Note:

If you enable or disable support for Hello messages, or change the listener port number, you must restart the RCS.

Configuration Scripts Tab

The Configuration Scripts tab lets you define scripts that the RCS will run automatically.

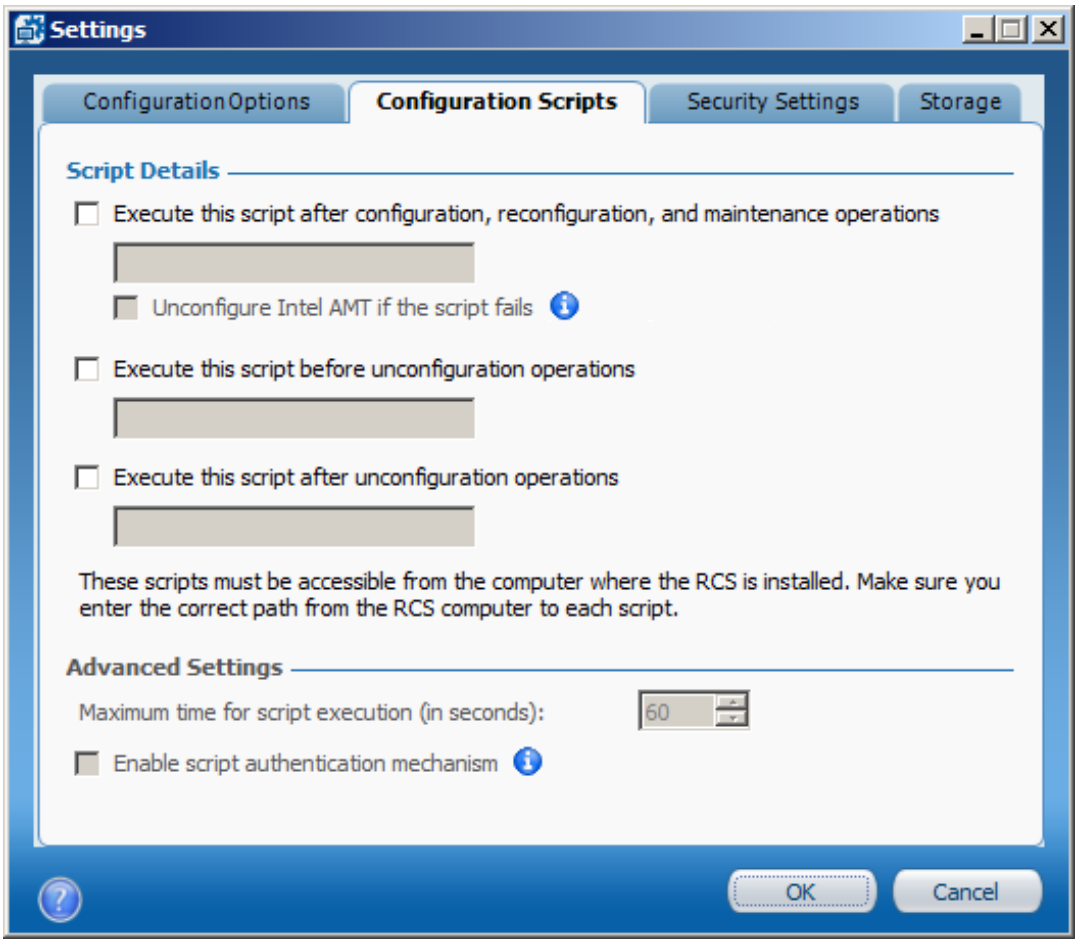


Figure 4-3: Configuration Scripts Tab

Script Details

Select the check box for each script that you want the RCS to run. You can select to run scripts:

- After configuration, reconfiguration and maintenance operations
- Before unconfiguration operations
- After unconfiguration operations

For each check box that you select, specify the full path to the script. These scripts must be accessible from the computer where the RCS is installed. Make sure that you enter the correct path from the RCS computer to each script. For more information about scripts, see Running Scripts with the Configurator/RCS on page 148.
For information about the **Unconfigure Intel AMT if the script fails** check box, see What if a Failure Occurs? on page 152.

Advanced Settings

You can use these settings to change the default behavior of the RCS when running scripts:

- **Maximum time for script execution (in seconds)** – See Script Runtime and Timeout on page 153
- **Enable script authentication mechanism** – See Script Authentication Mechanism on page 153

Security Settings Tab

The Security Settings tab includes optional security related settings.

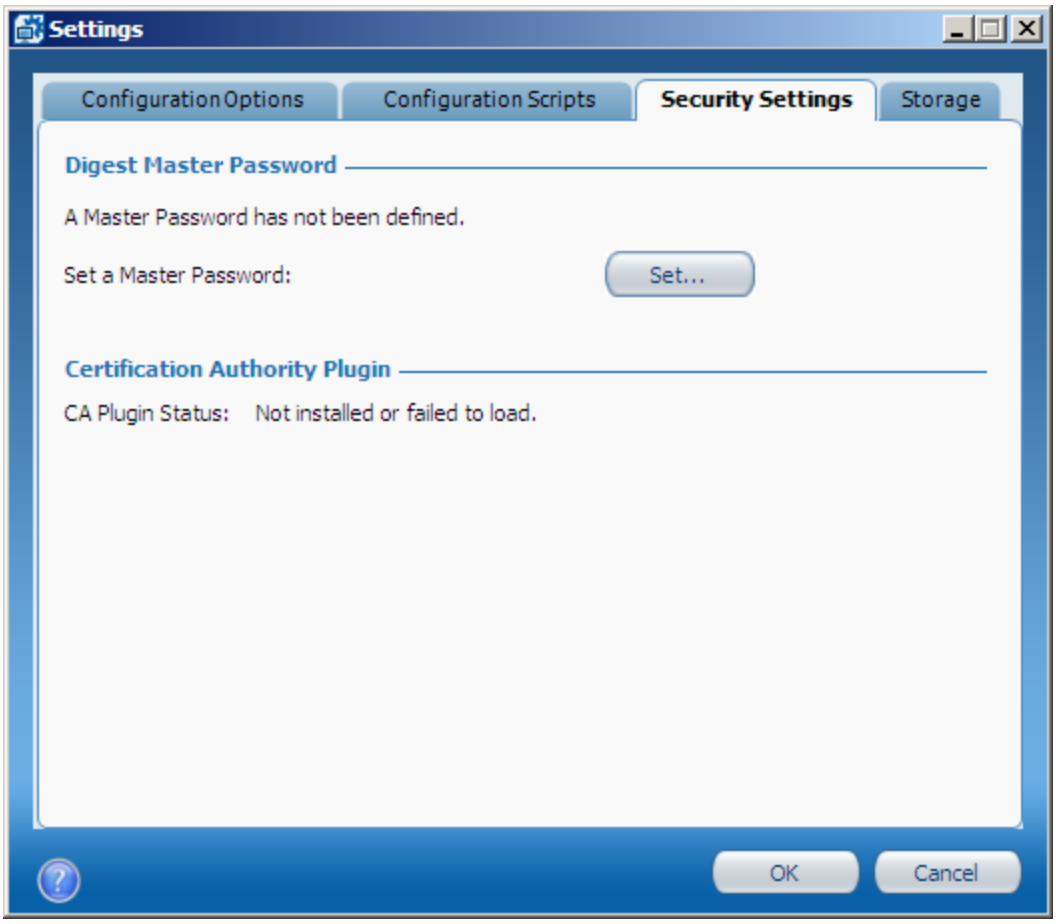


Figure 4-4: Security Settings Tab

Digest Master Password

To define the active Digest Master Password (DMP), click **Set** and enter the password. The password must be between 8-32 characters, with at least one number, one non-alphanumeric character, one lowercase Latin letter, and one uppercase Latin letter.

For increased security, change the DMP at regular intervals and then reconfigure the systems. The RCS saves the last 10 DMPs that were set in an encrypted file. If the file is full, when a new DMP is set the oldest entry is deleted.

Note:

For more information about this option and when to use it, see Admin Permissions in the Intel AMT Device on page 18. Keep a record of each DMP you set. You might need to supply them to third-party applications.

Certification Authority Plugin

This section shows the status of the optional CA plugin, as reported by the RCS.

For more information, see Using Intel SCS with the CA Plugin on page 204.

Storage Tab

The Storage tab contains settings that define where the RCS stores data and how that data is encrypted.

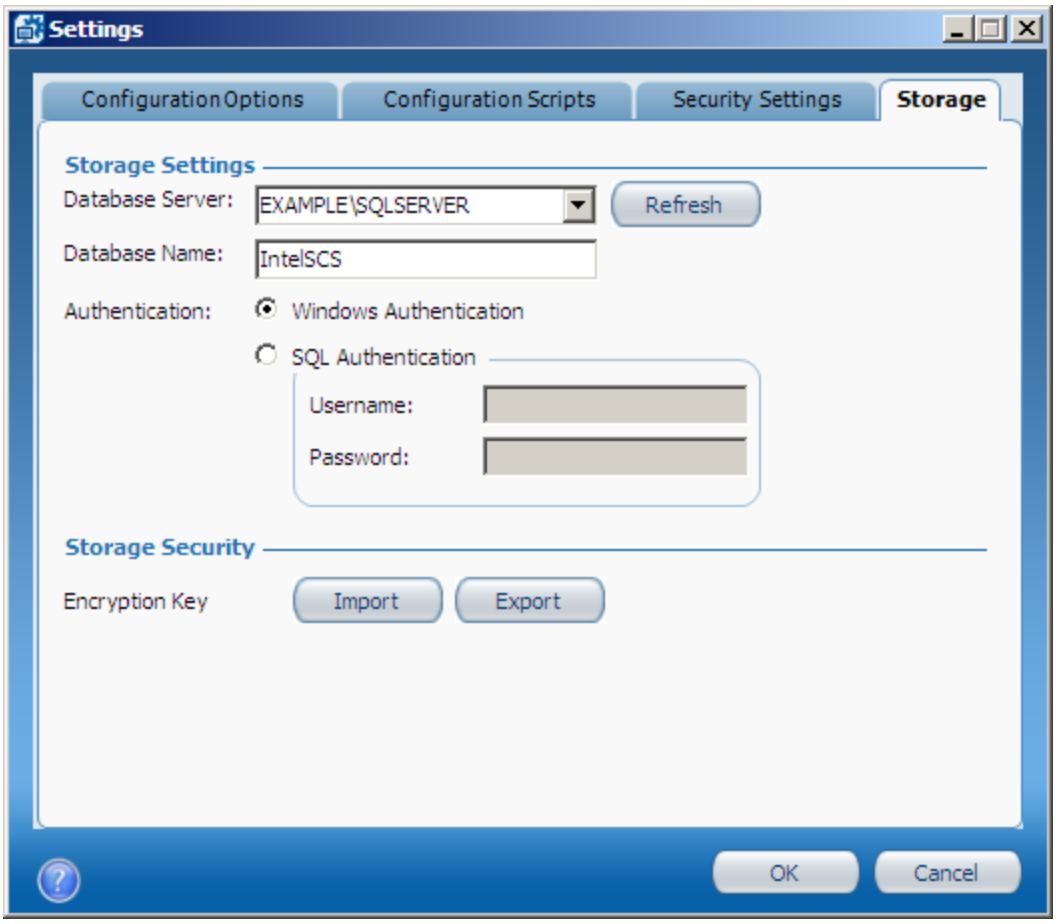


Figure 4-5: Storage Tab

Storage Settings

These settings are only shown if the RCS is in database mode. Only make changes to these settings if you want the RCS to connect to a different SQL database.

For more information, see Changing the Database on page 58.

Storage Security

The Import and Export buttons are used to import and export the encryption key. Only use these options if you want to backup the encryption key or move the RCS to a different computer.

For more information, see Moving the RCS to a Different Computer on page 58.

4.4 Creating Configuration Profiles

To define a configuration profile, do the following:

1. In the Console, click **Profiles** and then click  . The Profile Wizard window appears.

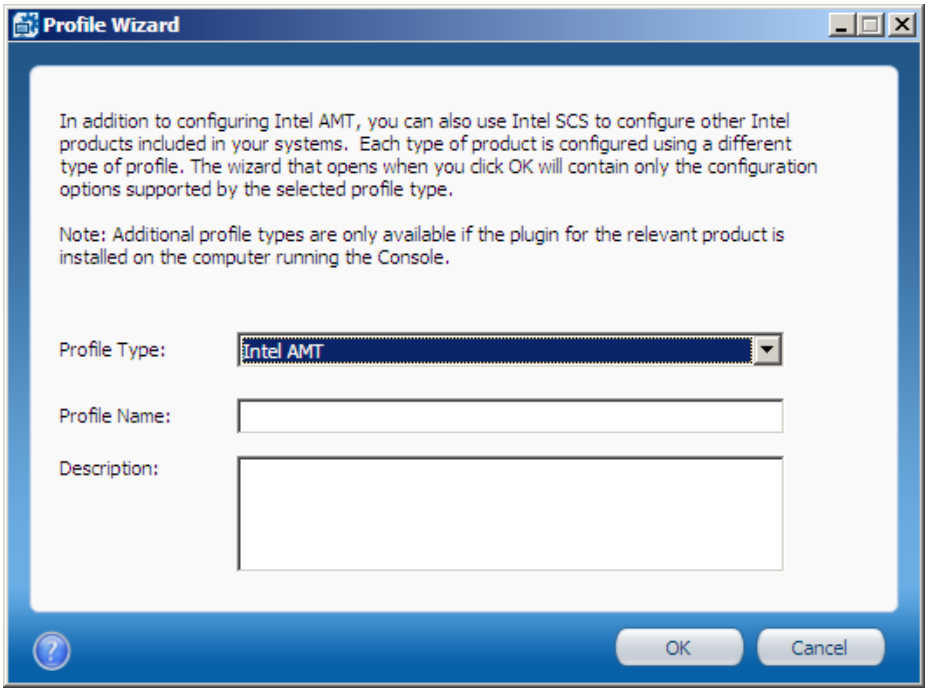


Figure 4-6: Profile Wizard Window

2. In the Profile Name field, type a name for this profile. The profile name
   - Can be a maximum of 32 characters
   - Cannot be empty or include only "whitespace" characters
   - Must include only alpha-numeric characters (7-bit ASCII characters in the range of 33-126), not including these characters:

     (/), (\ ), (:), (*), (?), (<), (>), (.), (,), (&), ("), (`), (|)
3. (Optional) In the Description field, type a description for the profile. This field is for informational purposes only.
4. Click **OK**. The relevant wizard or profile settings page for the selected profile type appears.
5. Select the settings that you want to configure when using this profile.

> **Note:**
>
> The fields and options that are shown will be different for each type of profile. For information about the available options, click the help icon.

6. Close the wizard/settings page. The profile is added to the list of profiles in the left pane of the Profiles tab. The profiles are grouped together by profile type (Intel AMT/solution).

4.5 Exporting Profiles from the Console

To use unified configuration (see Unified Configuration Process on page 9) you must export the Intel AMT profile in the Console to an XML file. You must then put this exported profile in your deployment package.

To export the profile:

1. In the Console, click **Profiles** and then select the Intel AMT profile you want to use to configure the systems.
2. Click **Export to XML**. The Export Profile to XML File window opens.

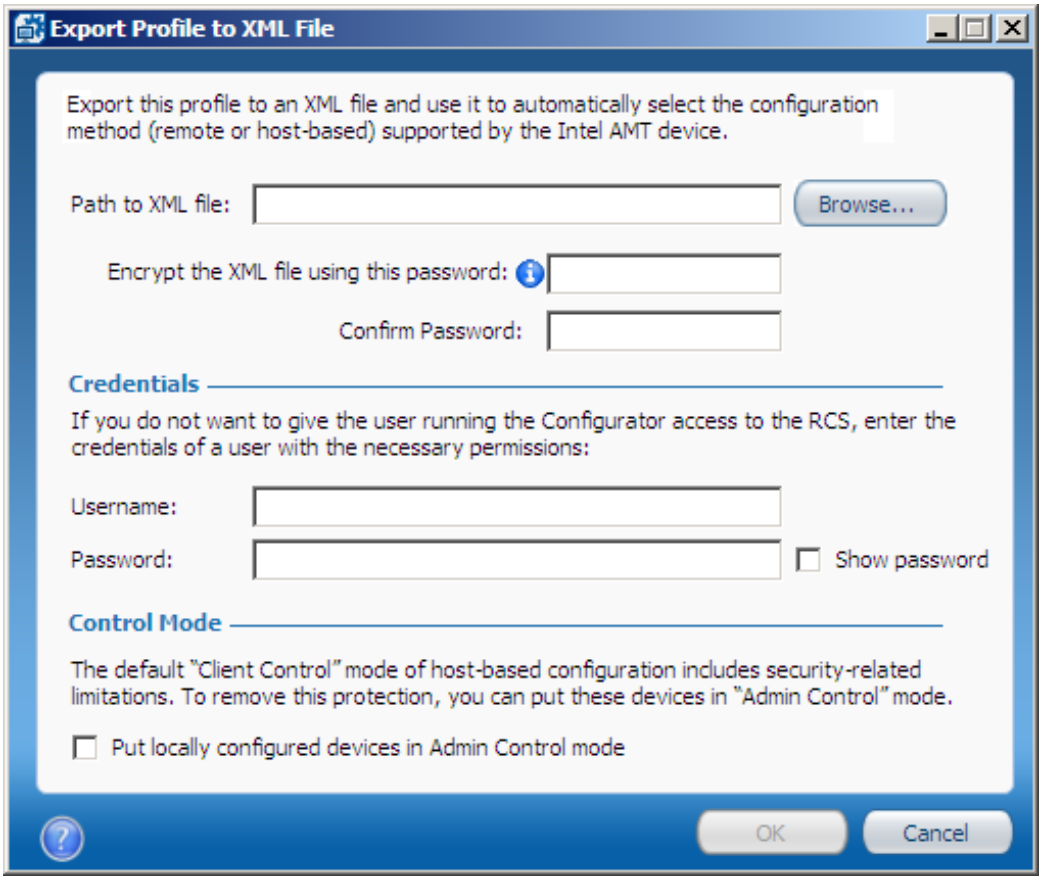


Figure 4-7: Export Profile to XML File Window

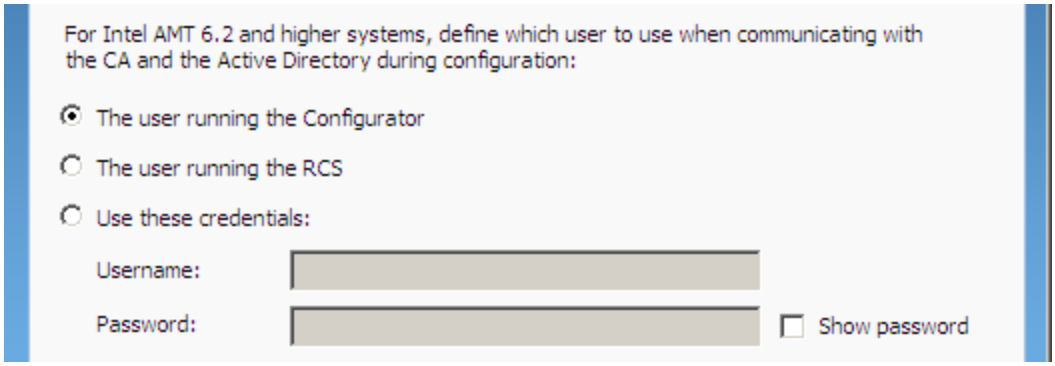
3. In the Path to XML file field, define a name and location for the exported file.

4. In the Encrypt the XML file using this password field, enter a password that will be used to encrypt the profile. For information about the required format, see Password Format on page 11.

> **Note:**
>
> Remember this password. You will need to supply it to the Configurator in the CLI command (using the `/DecryptionPassword` parameter).

5. (Optional) If you enter credentials of a user in the Username and Password fields, the Configurator will use that user to communicate with the RCS. (By default, the credentials of the user running the Configurator are used.) Use this option only if you do not want to give the Configurator WMI permissions on the RCS. For more information, see User Permissions Required to Access the RCS on page 52.
6. If the profile includes any of these settings:
   - Active Directory (AD) Integration
   - Requesting certificates from a Certification Authority (CA)

   these fields are shown in the Credentials section:



   To configure AD integration, the Configurator must send a request to the AD to create an AD object for the Intel AMT system. To configure certificates via the CA, the Configurator must request the certificate from the CA.

   You can define which user to use when making these requests:

   - **The user running the Configurator** – The Configurator sends the request directly to the CA/AD.
   - **The user running the RCS** – The Configurator sends the requests to the RCS. The RCS communicates with the CA/AD and sends the data returned by the CA/AD to the Configurator.
   - **Use these credentials** – The Configurator uses the supplied user credentials to send the request to the CA/AD.

> **Note:**
>
> - These options are only applicable for Intel AMT 6.2 and higher systems. For all other systems, the RCS is always used to communicate with the CA/AD.
> - Make sure that the user you define has the necessary permissions to communicate with the CA/AD.
> - In all cases, the configuration necessary in the Intel AMT device is done locally by the Configurator (Intel AMT 6.2 and higher only).

7. By default, Intel AMT 6.2 and higher devices are put in the Client Control mode (see Control Modes on page 15). If you need to remove the restrictions of Client Control mode, select **Put locally configured devices in Admin Control mode**. If you select this check box, the devices are put in Admin Control mode. This setting is ignored for Intel AMT versions earlier than 6.2.

> **Note:**
>
> Selecting this option is not supported by LAN-less systems (see Configuration of LAN-less Platforms on page 7).

4.6 Importing PSK Keys from a File

If the manufacturer has installed PSK keys in the Intel AMT devices, you can configure them remotely. The manufacturer must supply you with a Setup.bin file containing the PSK keys that were installed in the devices. After the keys are imported into the RCS, you can use the Configurator to configure the systems remotely.

To import keys from a file:

1. Before you can import the keys into the RCS, the Console must be connected to the RCS (see Connecting to the RCS on page 76).
2. Select **Tools** > **Import PSK Keys from File**. The Open window opens.
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 shows with details of how many keys were successfully imported.

> **Note:**
>
> If the file contains invalid or corrupted records, the keys will not be imported. Only keys that do not exist in the RCS are imported.

Chapter 5

Defining Intel AMT Profiles

This chapter describes how to define configuration profiles for Intel AMT. The information in this section is only relevant for Intel AMT profiles.

For more information, see:

5.1 About Intel AMT Profiles

Intel AMT profiles contain the configuration settings that will be put in the Intel AMT device during configuration. These profiles can be created and used by several of the Intel SCS components. These are the main types of Intel AMT profile:

- **Console Profiles** – These profiles are created and edited using the Console. The settings in these profiles are used when a configuration request is sent to the RCS.
- **Exported Profiles** – These profiles are created and edited using the Console and then "Exported" to an XML format. During export, the `<RCSParameters>` tag is added with information about the location of the RCS. These profiles can then be used by the Configurator as part of the Unified Configuration Process on page 9.
- **Delta Profiles** – A Console Profile and an Exported Profile can be a Delta Profile. After a system is configured, Delta Profiles can be used to make changes to specific settings only. The new settings in the Delta Profile will delete and replace the existing settings. Settings that are not defined in the Delta Profile will stay in their current condition on the systems.

Note:

- The Manual Configuration method does not use configuration profiles.
- The Intel AMT Configuration Utility can also be used to create XML configuration profiles. But, the profiles can only be used to configure systems that have Intel AMT 6.2 and higher.

About Deleting and Modifying Profiles

When you configure an Intel AMT system, the system is configured with the settings that exist in the configuration profile at the time of configuration. A profile does not contain a version number. This means that:

- A profile in the Console is only a "reference". You cannot guarantee that systems configured with a profile were configured with the current settings shown in the profile.
- When a configuration request is sent to the RCS, the current settings in the profile defined in the request are used to configure the system. Configuration requests containing a profile that was deleted from the Console will fail.
- In database mode, when a job is started the selected profile (for Configuration or Maintenance operations) is loaded into memory. The operation will run on all the systems with the profile settings that existed when the job was started. The job will continue to run with these profile settings on all systems defined in the job, even if you modify or delete the profile. If the RCS crashes, the profile is reloaded into memory when the RCS restarts. After the RCS restarts, operations on the remaining systems will fail (if the profile was deleted) or use the new profile settings (if the profile was modified).

5.2 Creating a Configuration Profile for Intel AMT

This procedure describes how to create an Intel AMT configuration profile.

To create a configuration profile for Intel AMT:

1. In the Console, click **Profiles** and then click  . The Profile Wizard window opens.
2. From the Profile Type drop-down list, select **Intel AMT**.
3. In the Profile Name field, enter a name for this profile. The profile name:
   - Can be a maximum of 32 characters
   - Cannot be empty or include only "whitespace" characters
   - Must contain only alpha-numeric characters (7-bit ASCII characters in the range of 33-126), not including these characters:

   (/), (\ ), (:), (*), (?), (<), (>), (.), (,), (&), ("), (`), (|)
4. (Optional) In the Description field, enter a description for the profile. This field is for informational purposes only.
5. Click **OK**. The Getting Started window of the Configuration Profile Wizard opens.

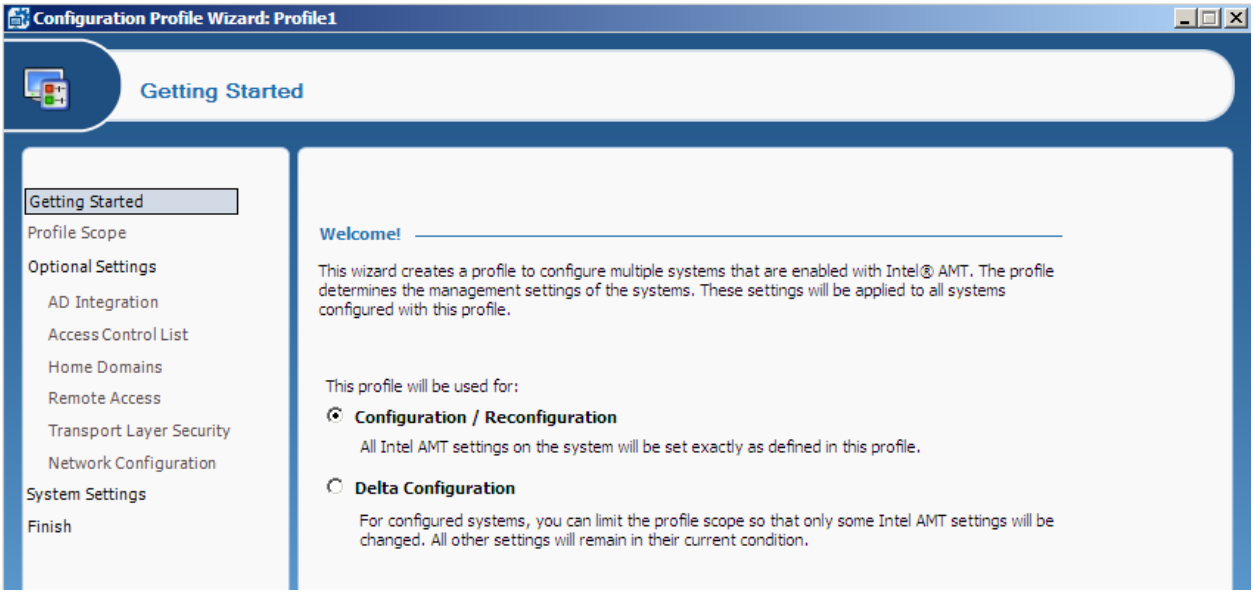


Figure 5-1: Getting Started Window

6. Select the task for which you want to use this profile:
   - **Configuration / Reconfiguration** – Systems configured using this profile will be set with the Intel AMT settings exactly as they are defined in this profile. Optional settings that are not defined in this profile will be removed from the systems during configuration.
   - **Delta Configuration** – After a system is configured, you can use this option to make changes to specific settings only. Only settings defined in the Profile Scope window will be changed on the systems during configuration. (The new settings will delete and replace the existing settings.) Settings that are not selected in the Profile Scope window will stay in their current condition on the systems.
7. Click **Next** to continue in the Configuration Profile Wizard and define the settings as described in these topics:
   - Defining the Profile Scope on the next page
   - Defining Profile Optional Settings on page 91
     - Defining Active Directory Integration on page 92
     - Defining the Access Control List (ACL) on page 95
     - Defining Home Domains on page 99
     - Defining Remote Access on page 100
     - Defining Transport Layer Security (TLS) on page 107
     - Defining Network Setups on page 110
   - Defining System Settings on page 119
8. When you have defined all the settings for this profile, the Finish window opens. Click **Finish** to save the profile.

5.3 Defining the Profile Scope

The Profile Scope window of the Configuration Profile Wizard lets you limit the settings that will be configured on systems when using this profile.

> **Note:**
>
> The Profile Scope window is only shown in delta configuration profiles.

Only settings defined in the Profile Scope window will be changed on the systems during configuration. (The new settings will delete and replace the existing settings.) Settings that are not selected in the Profile Scope window will stay in their current condition on the systems. Thus, you can use this profile:

- To configure systems without making changes to Intel AMT settings configured using third-party applications
- To make changes to specific Intel AMT settings on configured systems

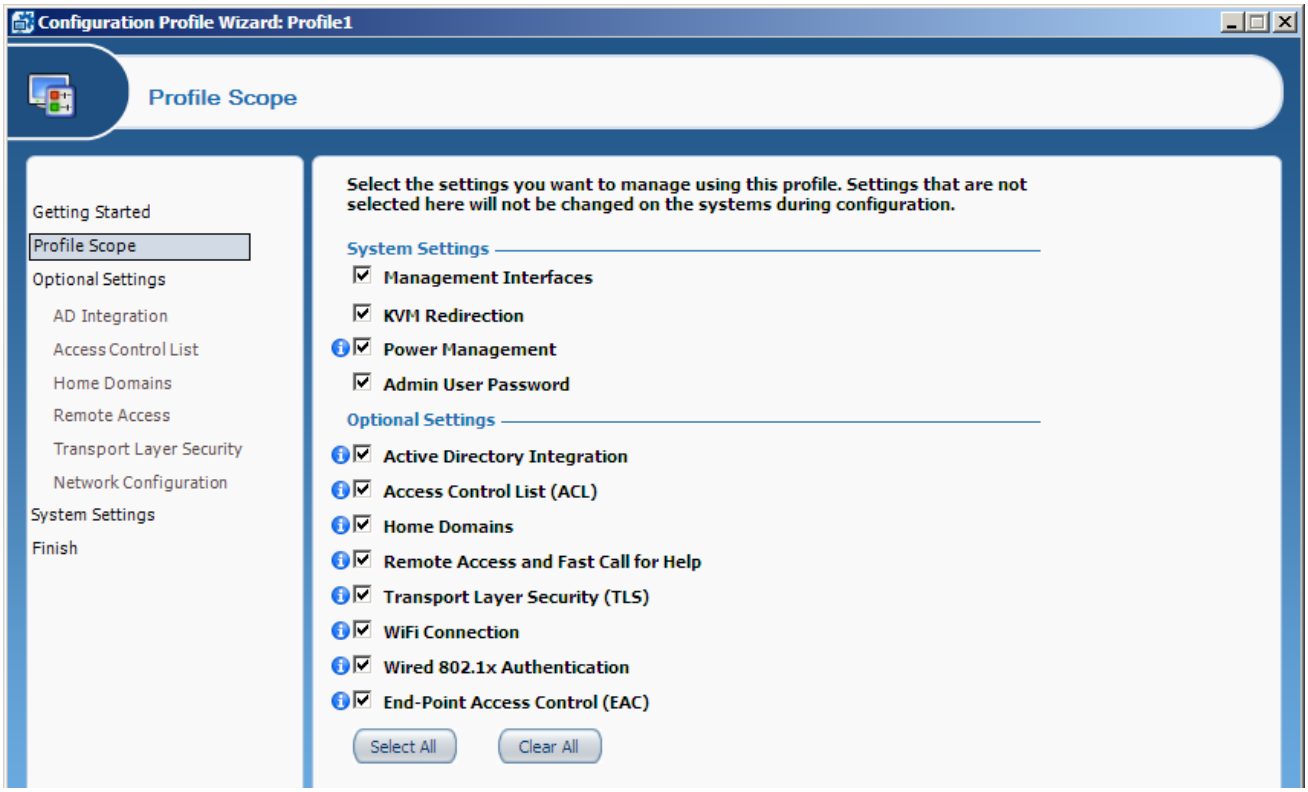


Figure 5-2: Profile Scope Window

To limit the profile scope:

1. Select the check boxes of all the settings that you want to configure/unconfigure on the systems using this profile. Settings that are not selected will not be shown in the Configuration Profile Wizard when you continue to edit the profile.
2. Click **Next** to continue to the Optional Settings window.

5.4 Defining Profile Optional Settings

The Optional Settings window of the Configuration Profile Wizard lets you select which optional settings to configure/unconfigure in the Intel AMT device using this profile.

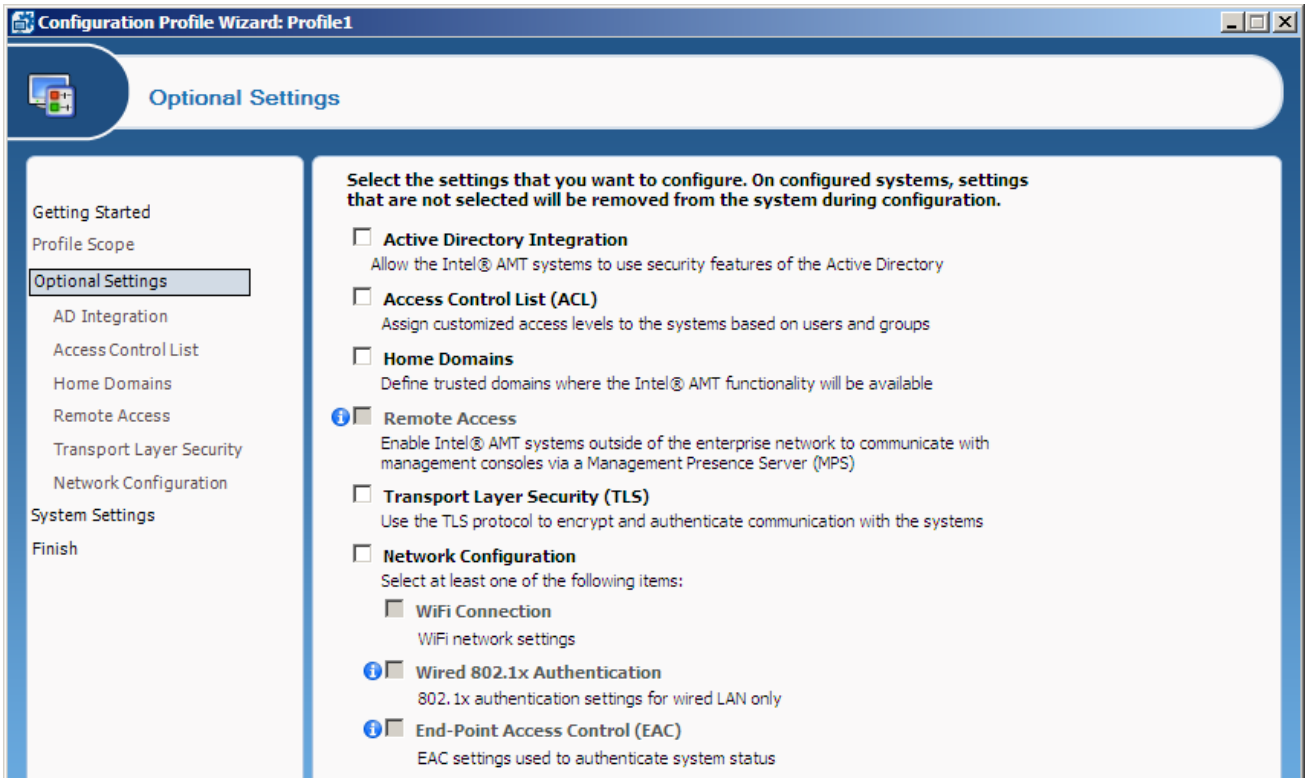


Figure 5-3: Profile Optional Settings Window

To select the optional settings:

1. Select the check boxes of the optional settings you want to configure using this profile. Intel SCS will remove (unconfigure) any existing settings from the Intel AMT system of options that are not selected in this window.
2. Click **Next** to continue in the Configuration Profile Wizard and define the configuration settings, as described in these topics:
   - Defining Active Directory Integration on the next page
   - Defining the Access Control List (ACL) on page 95
   - Defining Home Domains on page 99
   - Defining Remote Access on page 100
   - Defining Transport Layer Security (TLS) on page 107 (enabled by default)
   - Defining Network Setups on page 110

5.5 Defining Active Directory Integration

The Active Directory Integration window lets you integrate Intel AMT with the security infrastructure of your network's Active Directory (AD). This integration includes the ability to:

- Use Domain user accounts for Kerberos authentication with the Intel AMT device
- Use the 802.1x protocol for wired and wireless access
- Use End-Point Access Control (EAC)

Figure 5-4: Active Directory Integration Window

To define Active Directory Integration:

- Click  and select the Active Directory Organizational Unit (ADOU) where the object will be stored in AD. During configuration, Intel SCS sends a request to the AD to create a Computer object representing the Intel AMT device. The object is added to the ADOU you defined in this field.

This is the only setting that is required to activate AD integration for Intel AMT. The remaining settings in this window are optional, and can only be selected after defining the ADOU.

Note:

For information about the **Always use the OS Host Name for the new AD Object** check box, see Disjointed Hostnames and AD Objects on page 224.

For more information about the remaining optional settings, see:

- Defining Additional Security Groups on the next page
- Defining Additional Object Attributes on page 94

5.5.1 Defining Additional Security Groups

The AD Object created for the Intel AMT device is by default automatically added to the AD Security group named "Domain Computers". If necessary, it is also possible to define additional Security groups to which the object will be added. For example, some RADIUS servers require objects to be members of a specific Security group.

To add the object to additional Security groups:

1. Next to the Specify any additional Security groups for the object field, click  . The Active Directory Security Groups window opens.

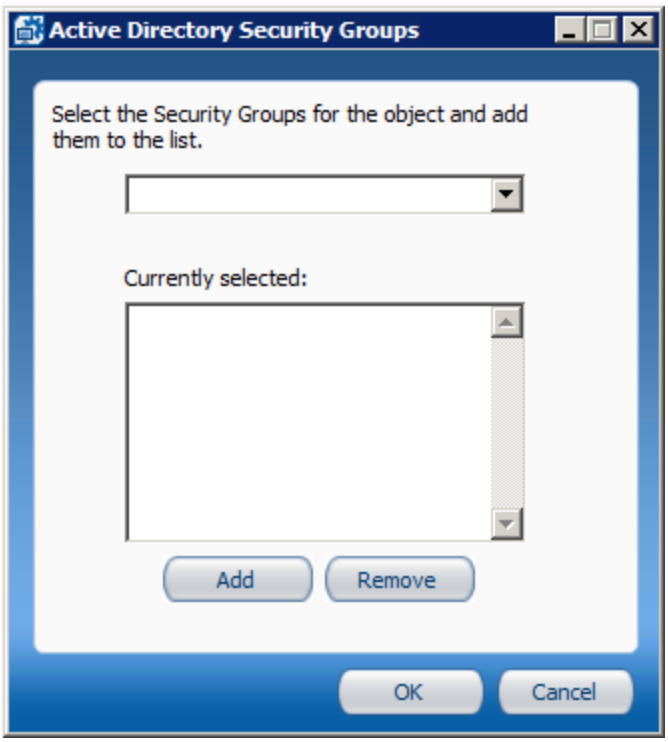


Figure 5-5: Active Directory Security Groups Window

2. From the drop-down list, select a Security group and click **Add**. The group is added to the list.
3. If required, repeat step 2 to add additional Security groups to the list.
4. Click **OK**. The Active Directory Security Groups window closes.

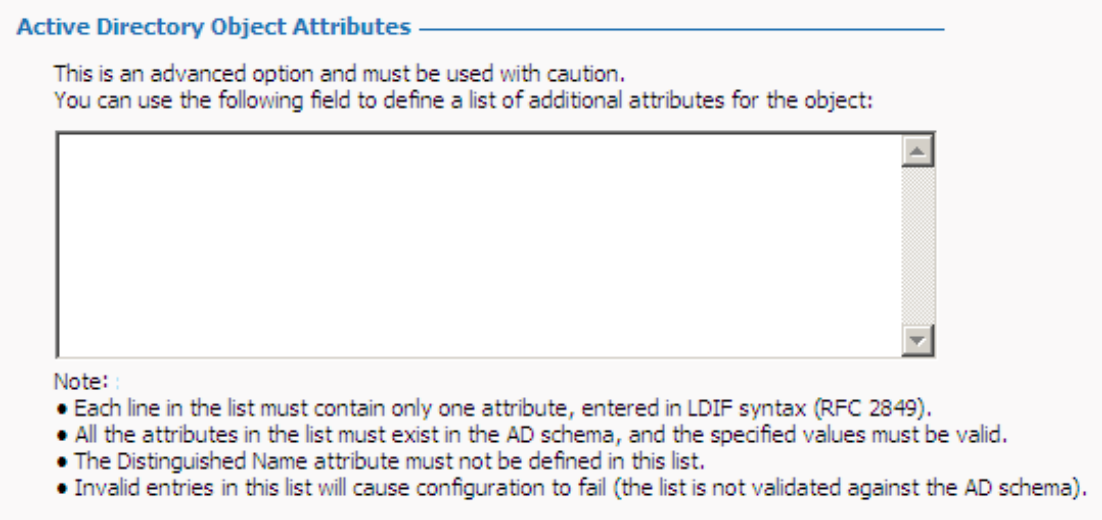
5.5.2 Defining Additional Object Attributes

The object created for the Intel AMT device is automatically assigned all the attributes and values necessary for AD integration. If necessary, you can also define additional attributes and values for the AD object.

> **Note:**
>
> You can only define attributes of the "String" type.

To define additional object attributes:

1. Click **Advanced**. This additional field is shown:



2. In the text field, define the list of attributes and values that you want to add to the object. Each line in the list must contain only one attribute, entered in the Lightweight Directory Interchange Format (LIDF) described in RFC 2849.

   For example:

   ```
   attributeName1: attributeValue1

   attributeName2: attributeValue2
   ```

3. When the list is complete, click **Next** to continue. If the list contains invalid entries, an error message will show the lines with the invalid syntax.

> **Note:**
>
> - All the attributes in the list must exist in the AD schema, and the specified values must be valid
> - The Distinguished Name attribute must NOT be defined in this list
> - Invalid entries in this list will cause configuration to fail. The list is not validated against the AD schema.
> - If the list includes attributes configured by Intel SCS, the value defined in the list will replace the value usually configured by Intel SCS.

5.6 Defining the Access Control List (ACL)

The Access Control List (ACL) window of the Configuration Profile Wizard lets you define users and their access privileges in the Intel AMT device. If you enable ACL, you must define at least one user or group, but no more than seven digest users and 32 Active Directory users/groups. User identification and realm selection must be coordinated with the requirements and instructions of third-party management consoles.

Figure 5-6: Access Control List (ACL) Window

You can do these tasks to define the users in the ACL:

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

Note:

During configuration, all the existing user accounts defined in Intel AMT are replaced with the user accounts defined in the profile in this ACL window. This means that the ACL list must always contain the full list of user accounts that you want to configure in Intel AMT.

5.6.1 Adding a User to the ACL

The User/Group Details window lets you add a new user or user 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 opens.

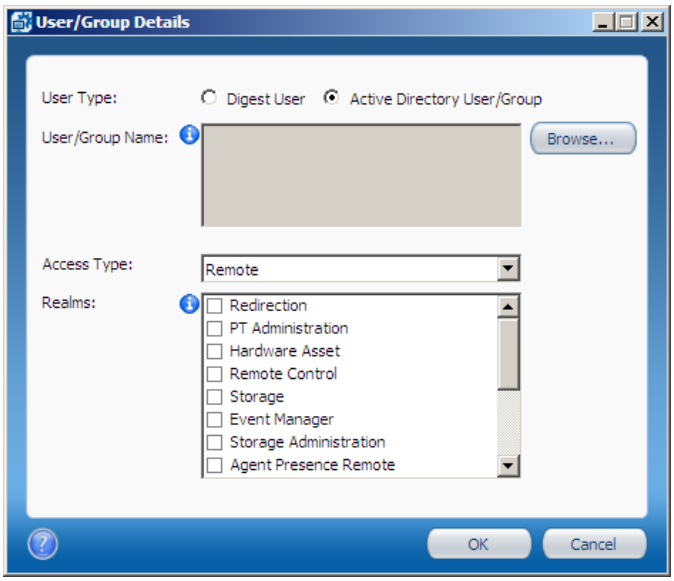


Figure 5-7: User/Group Details Window

2. In the User Type section, select the required type of user:
   - **Digest User** – Enter the username and password (see Password Format on page 11). The usernames "admin" and "administrator" are not permitted (these names are reserved for the default admin user). The username must be unique in this profile, a maximum of 16 characters, and cannot contain these characters:

     (,), (:), ("), (&), (<), or (>). Usernames starting with $$ are not permitted.
   - **Active Directory User/Group** – Click **Browse** and select the user or group.

> **Note:**
>
> You cannot 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 do an action. A user might be limited to local actions or might also be able to do actions from the network. Select one of these:
   - **Local** – The user can access the Intel AMT system only via the local host.
   - **Remote** – The user can execute an action only via the network.
   - **Both** – The user can execute an action either locally or from the network.

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, as described in this table. Note that not all realms are available on all versions of Intel AMT.

   Table 5-1: Intel AMT Realms

Realm	Capabilities
Redirection	Enables and disables the redirection capability and retrieves the redirection log
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. **Note:** If this user will be used to run the Configurator to do host-based configuration, the Access Type must be **Local** (or **Both**).
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
Event Manager	Allows configuring hardware and software events to generate alerts
Storage Administration	Used to configure the global parameters that govern the allocation and use of non-volatile storage
Agent Presence Local	Used by an application designed to run on the local platform to report that it is running and to send heartbeats periodically
Agent Presence Remote	Used to register Local Agent applications and to specify the behavior of Intel AMT when an application is running or stops running unexpectedly
Circuit Breaker	Used to define filters, counters, and policies to monitor incoming and outgoing network traffic and to block traffic when a suspicious condition is detected (the System Defense feature)
Network Time	Used to set the clock in the Intel AMT device and synchronize it to network time
General Info	Returns general setting and status information. With this interface, it is possible to give a user permission to read parameters related to other interfaces without giving permission to change the parameters
Firmware Update	Used only by manufacturers via Intel-supplied tools to update the Intel AMT firmware

Realm	Capabilities
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/NAP posture
Endpoint Access Control Administrator	Configures and enables the NAC/NAP 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 below.
User Access Control	Groups several ACL management commands into a separate realm to enable users to manage their own passwords without requiring administrator privileges

5.6.2 Using Access Monitor

The access monitor serves as a deterrent to rogue administrator activity by tracing attempts to execute 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.

5.7 Defining Home Domains

The Home Domains window of the Configuration Profile Wizard lets you define a list of between one and five home domains. If configured, these home domains are the only domains in which access to Intel AMT is permitted. When Intel AMT detects that the systems is located outside these home domains, remote access to Intel AMT is blocked.

> **Note:**
>
> Configuring a system with incorrect home domains might cause remote access to Intel AMT to be permanently blocked. If this occurs, it will also not be possible to remotely reconfigure Intel AMT on these systems.

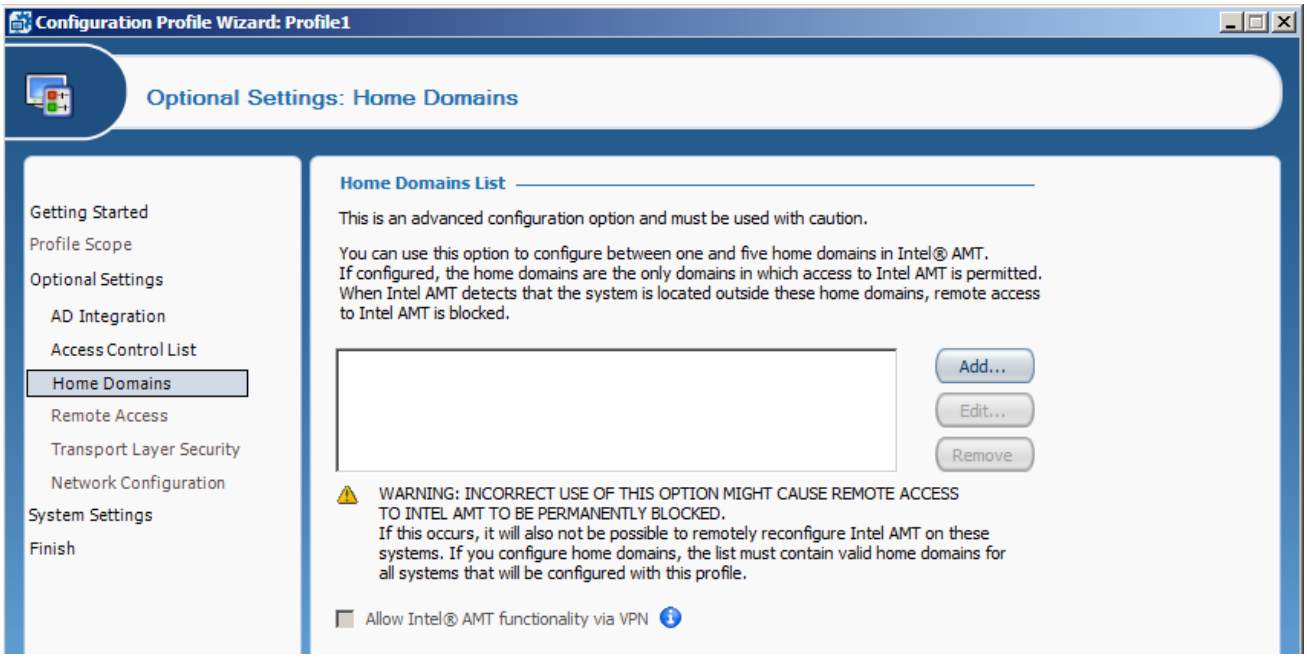


Figure 5-8: Home Domains Window

To define the domains:

1. Click **Add**. The Domain Properties window opens.
2. Enter the DNS suffix name and click **OK**. The Domain Properties window closes and the domain is added to the list of home domains.

   > **Note:**
   >
   > Make sure that the list of home domains contains valid home domains for all systems that will be configured with this profile.

3. (Optional) To permit access to Intel AMT over a Virtual Private Network, select **Allow Intel® AMT functionality via VPN**. If selected, access to the Intel AMT system is permitted when it is connected over a VPN to a domain in the Home Domains list.

5.8 Defining Remote Access

The remote access feature lets Intel AMT systems located outside an enterprise connect to management consoles inside the enterprise network. The connection is established 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. Multiple consoles can interact with the Intel AMT device through the tunnel.

Note:

Intel SCS supports the capability available in Intel AMT to define the MPS. Intel SCS does not ship an MPS and does not endorse or recommend any 3rd party MPS server you may choose to use in your environment. Since Intel SCS cannot perform configuration through an MPS, you must configure your Intel AMT systems on-prem prior to utilizing this capability to manage those systems through the firewall.

For remote access to work, the Intel AMT system must first be configured when it is inside the enterprise with the information needed to connect with the MPS.

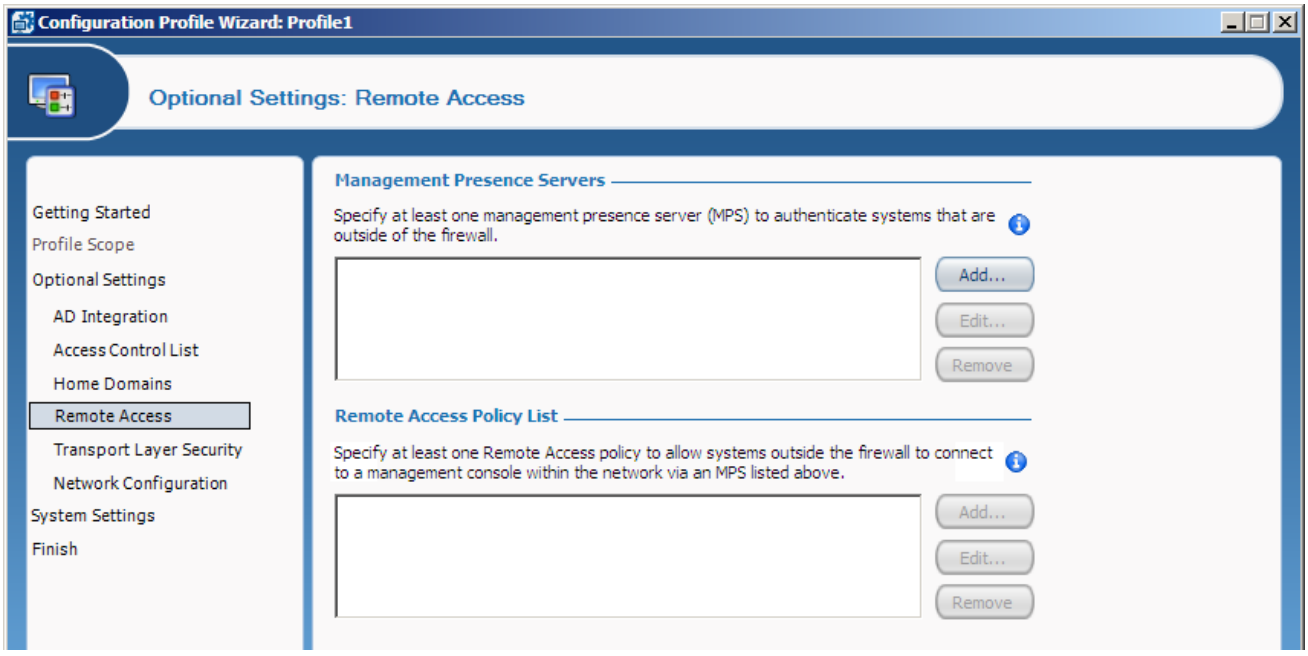


Figure 5-9: Remote Access Window

To define the remote access parameters, see these topics:

- Defining Management Presence Servers on the next page
- Defining Remote Access Policies on page 103

5.8.1 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 opens.

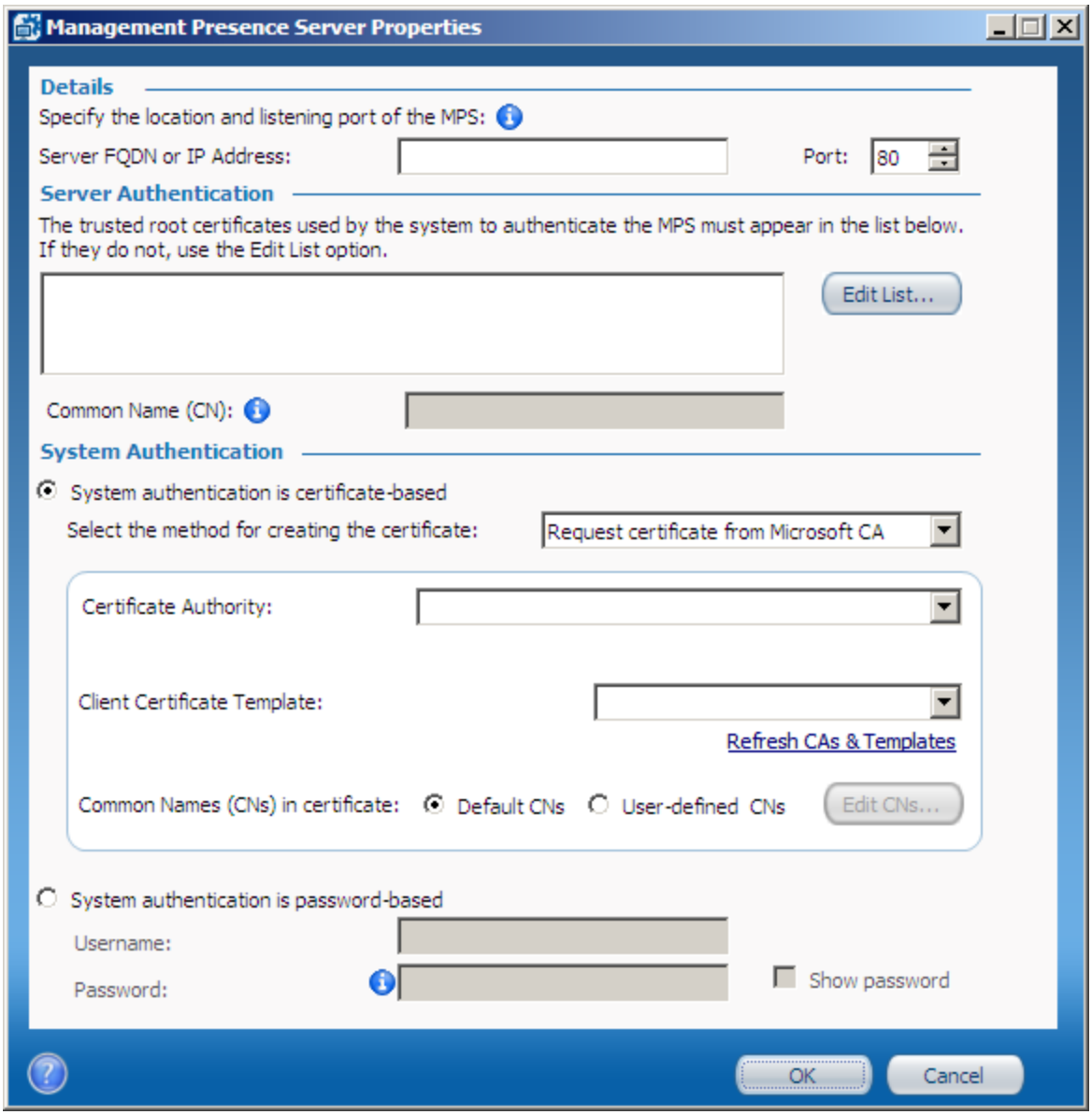


Figure 5-10: Management Presence Server Properties Window

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

4. Click **Edit List** to define the location of the trusted root certificates that will be used by Intel AMT systems configured with this profile (see Defining Trusted Root or Intermediate Certificates (CAs) on page 104).
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. Define the required type of authentication:
   - To define authentication based on a password, select **System authentication is password-based**, enter a username and password, and continue from step 9.
   - To define authentication based on certificates, select **System authentication is certificate-based**, and continue from step 7.
7. From the Select the method for creating the certificate drop-down list, select the source for the certificate that will be installed in the Intel AMT device:
   - **Request certificate from Microsoft CA** – By default, the settings for this option are displayed. If you are using a Microsoft* CA, continue to step 8.
   - **Request Certificate via CA plugin** – This option is only available if you have installed the optional CA plugin. For information about this option, see Using Intel SCS with the CA Plugin on page 204. If you select this option, enter the necessary settings (as defined by the plugin provider) and continue from step 9.
8. If the certificate will be requested from a Microsoft CA, do these steps:
   a. From the Certificate Authority drop-down list, select the Enterprise CA that Intel SCS will use to request a certificate that the MPS can authenticate.
   b. From the Client Certificate Template drop-down list, select the template that will be used to create the client certificate. The templates shown are templates where the Subject Name is supplied in the request and the usage is "Client Authentication". For information how to create a template, see Defining Enterprise CA Templates on page 192.
   c. Define the Common Names that will be included in the Subject Name of the generated certificate. For more information, see Defining Common Names in the Certificate on page 205.

   Note:

   - To use this option, Intel SCS must have access to the CA during configuration (see Required Permissions on the CA on page 200).
   - If you are creating the profile on a computer that does not have access to the CA, the drop-down lists will not display the CA or the templates. If necessary, you can manually supply the CA name (in the format FQDN\CA Name) and the name of the template.
9. Click **OK**. The settings are saved and the Management Presence Server window closes.

5.8.2 Defining Remote Access Policies

A Remote Access policy defines what will cause the Intel AMT device to establish a connection with an MPS (the trigger), and to which MPS it will connect. If Remote Access is enabled, 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 opens.

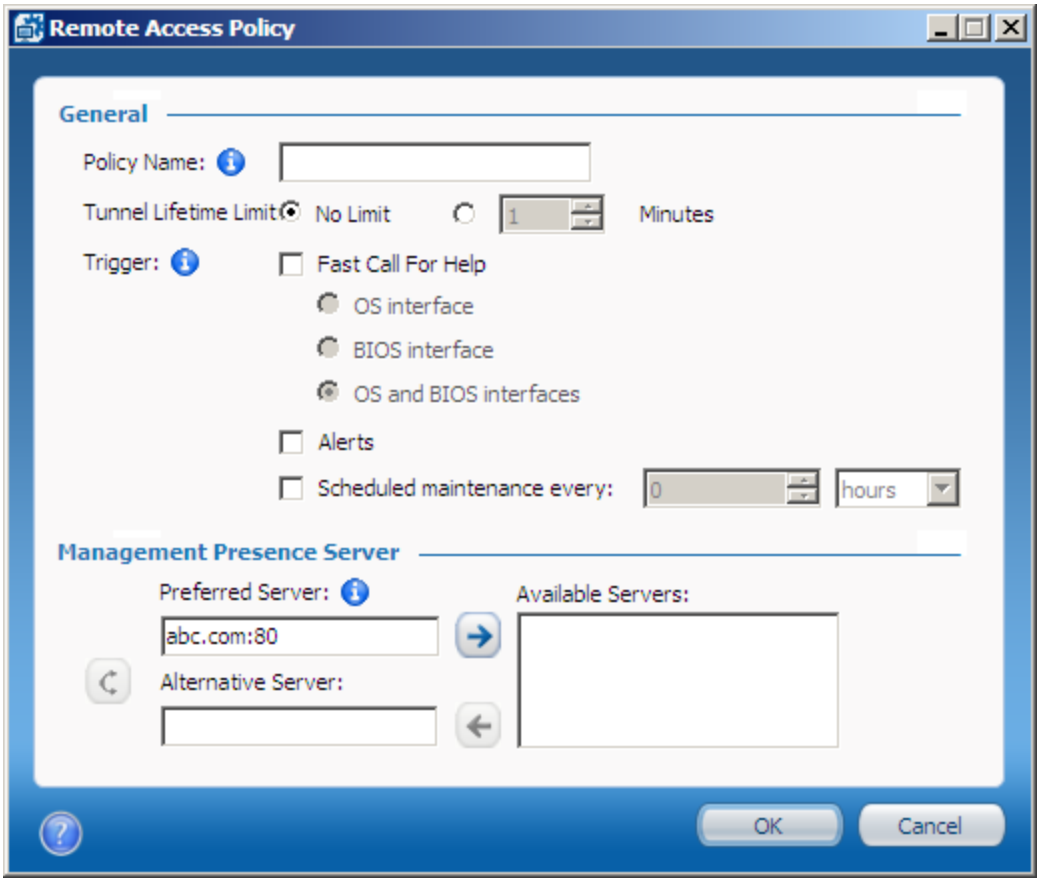


Figure 5-11: Remote Access Policy Window

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 for this policy:
   - **Fast Call For Help** – The Intel AMT device establishes a tunnel with the MPS when the user initiates a connection request. If required, you can limit when the user can access this option (only from the operating system or only from the BIOS). By default, both options are available to the user.
   - **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 two different policies cannot 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.

5.9 Defining Trusted Root or Intermediate Certificates (CAs)

An Intel AMT system must have a trusted root or intermediate certificate (CA) to use any of these features:

- Remote Access using a Management Presence Server
- Mutual authentication in Transport Layer Security
- Most types of 802.1x setups

To define the trusted root certificates:

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

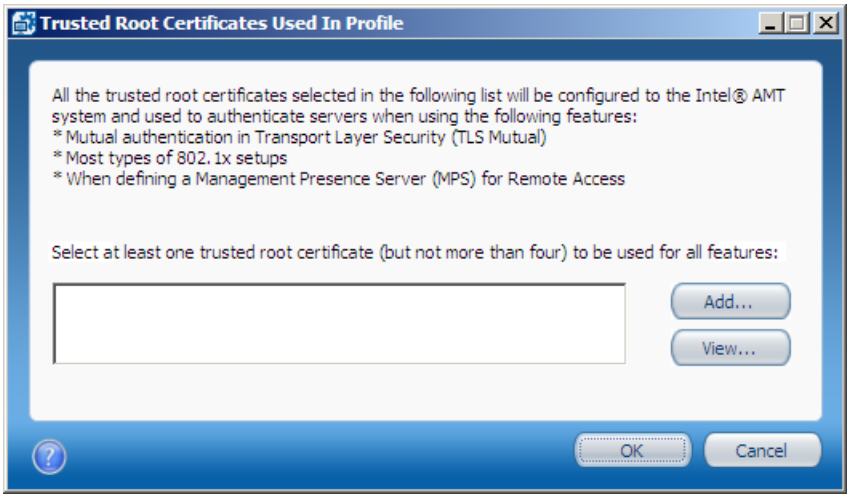


Figure 5-12: Trusted Root Certificates Used In Profile Window

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

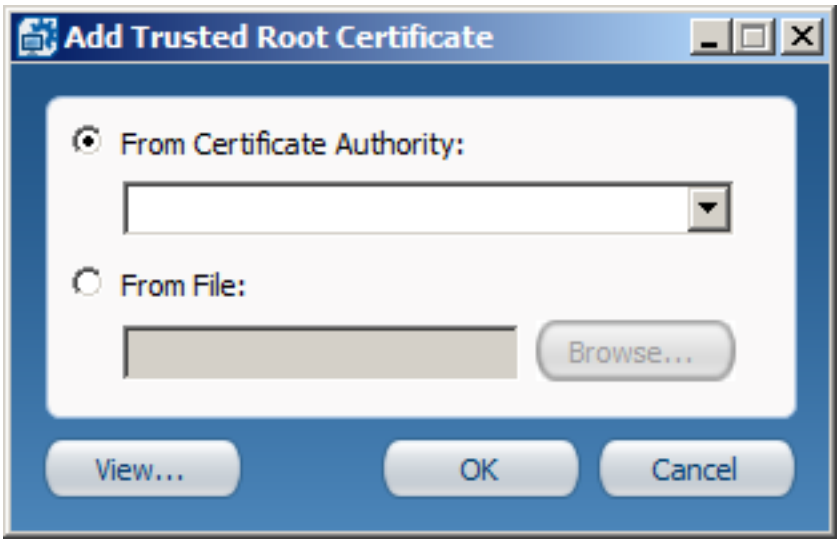


Figure 5-13: Add Trusted Root Certificate Window

3. Select one of these:
   - **From Certificate Authority** – From the drop-down list, select the Trusted Root Certification Authority (CA).
   - **From File** – Enter the path to the file or click **Browse** to locate and select a certificate. The file must be in base64 PEM format.

   Note:

   You can only add a certificate from a root or intermediate CA.

4. Click **OK**. The Path to Root Certificate window closes and the certificate shows 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.

5.10 Defining Transport Layer Security (TLS)

The Transport Layer Security (TLS) window of the Configuration Profile Wizard lets you define TLS settings to apply to the Intel AMT system.

Note:

TLS 1.0 has been deprecated as the security protocol for Intel SCS communication with Intel AMT. The TLS 1.0 protocol has identified security vulnerabilities, including CVE-2011-3389 and CVE-2014-3566. Intel SCS will default to TLS 1.1 or TLS 1.2 (depending on your Intel AMT version) to encrypt communication between Intel SCS software components and Intel AMT. Users can enable TLS 1.0 protocol support for backwards compatibility, both during installation of the Remote Configuration Server (RCS) and after installation/upgrade of the RCS.

When TLS is enabled, the Intel AMT device authenticates itself with other applications using a server certificate. 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.

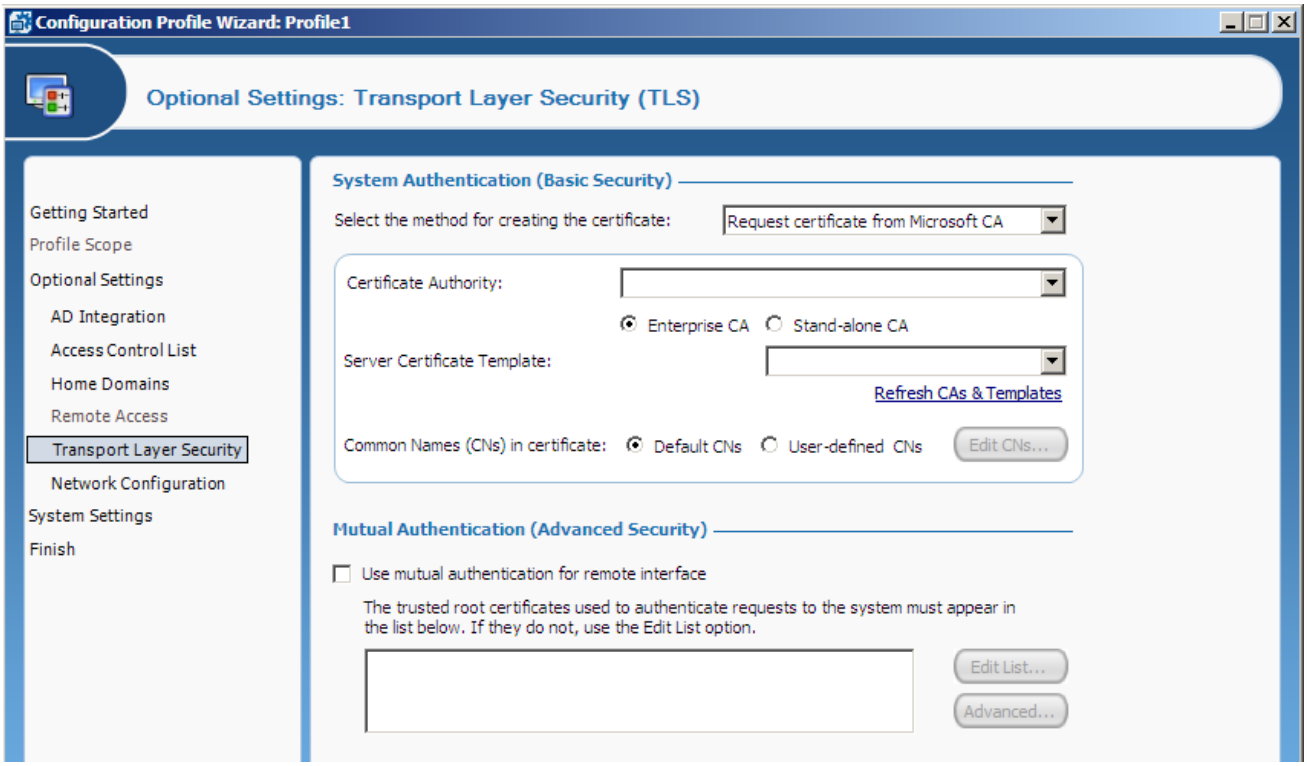


Figure 5-14: Transport Layer Security (TLS) Window

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 Select the method for creating the certificate drop-down list, select the source for the certificate that will be installed in the Intel AMT device:
   - **Request certificate from Microsoft CA** – By default, the settings for this option are displayed. If you are using a Microsoft* CA, continue to step 2.
   - **Request Certificate via CA plugin** – This option is only available if you have installed the optional CA plugin. For information about this option, see Using Intel SCS with the CA Plugin on page 204. If you select this option, enter the necessary settings (as defined by the plugin provider) and continue from step 3.
2. If the certificate will be requested from a Microsoft CA, do these steps:
   a. From the Certificate Authority drop-down list, select the certification authority. Intel SCS automatically detects if the selected CA is a Standalone CA or an Enterprise CA.
   b. If you are using an Enterprise CA, you must select the template that will be used to create the certificate. From the Server Certificate Template drop-down list, select the template that you defined for TLS. For information how to create a template for TLS, see step 15 of Defining Enterprise CA Templates on page 192.
   c. Define the Common Names that will be included in the Subject Name of the generated certificate. For more information, see Defining Common Names in the Certificate on page 205.

   Note:

   - To use this option, Intel SCS must have access to the CA during configuration (see Required Permissions on the CA on page 200).
   - If you are creating the profile on a computer that does not have access to the CA, the drop-down lists will not display the CA or the templates. If necessary, you can manually supply the CA name (in the format FQDN\CA Name) and the name of the template. When entering these values manually, you must also select the type of CA (Enterprise CA or Standalone CA).
3. (Optional) To enable mutual TLS:
   a. Select **Use mutual authentication for remote interface**.
   b. Define the trusted root certificates that will be used by Intel AMT systems configured with this profile (see Defining Trusted Root or Intermediate Certificates (CAs) on page 104).
   c. (Optional) Define advanced mutual TLS settings (see Defining Advanced Mutual Authentication Settings below).

5.10.1 Defining Advanced Mutual Authentication Settings

The Advanced Mutual Authentication Settings window lets you define a Certificate Revocation List (CRL). The CRL is a list of entries, usually supplied by a CA, that indicate which certificates have been revoked (see CRL XML Format on page 207 for the required format).

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 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, click **Advanced**. The Advanced Mutual Authentication Settings window opens.

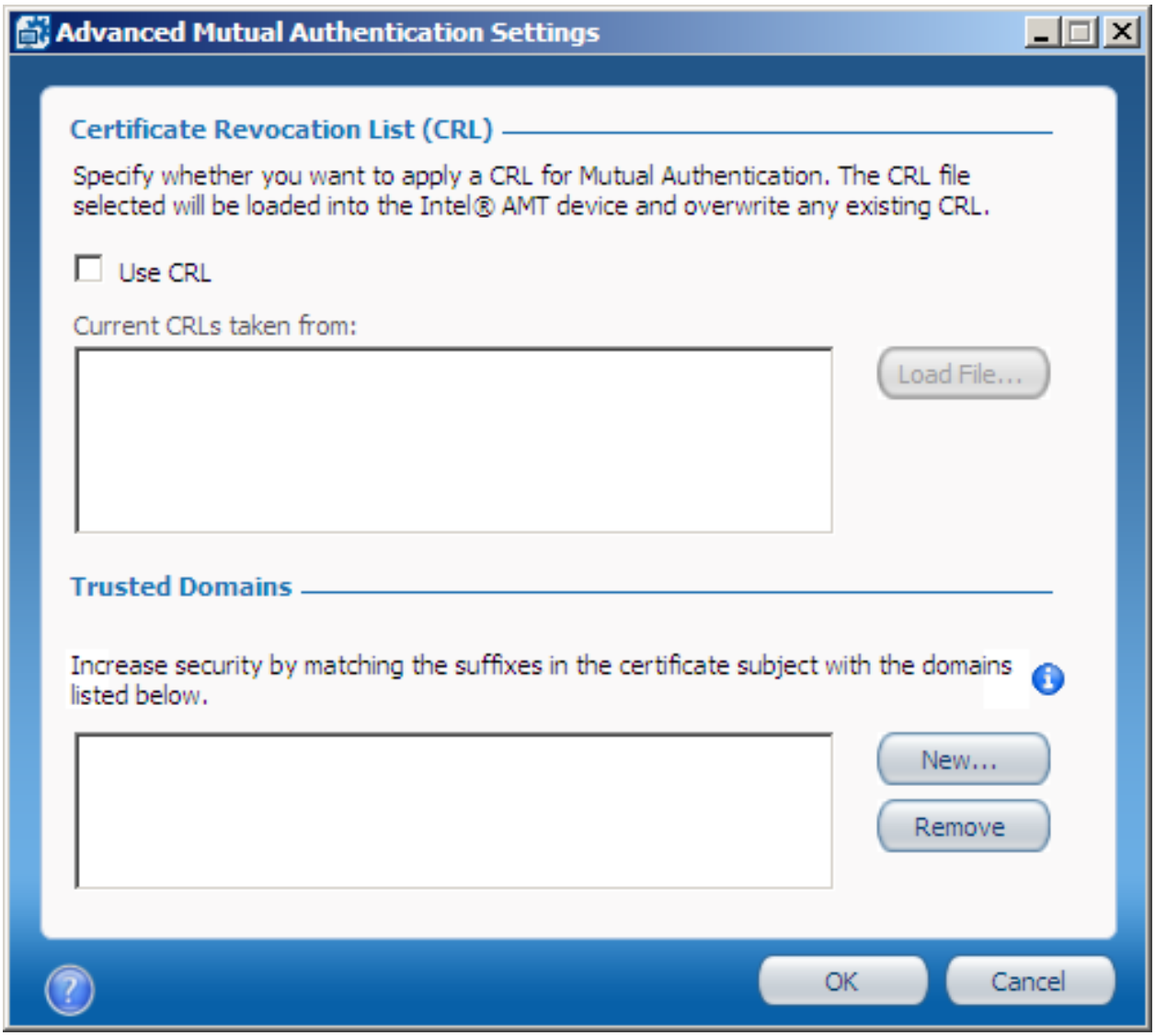


Figure 5-15: Advanced Mutual Authentication Settings Window

2. (Optional) Define the CRL you want to use in this profile:
   a. Select **Use CRL**.
   b. Click **Load File**. The Open window opens.
   c. Browse to the location of the CRL XML file, select it and click **Open**. The information in the file is imported into the configuration profile, and the name of the file is added to the list.

3. (Optional) 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 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.

5.11 Defining Network Setups

The Network Configuration window of the Configuration Profile Wizard lets you define several network setups that the Intel AMT device must use. A network setup includes encryption and authentication protocol settings and can be used for wired or wireless connections. If you define WiFi Connection settings in the profile, the wireless interface of Intel AMT is enabled during configuration.

Note:

Removing the WiFi Connection settings from a profile does not always disable the wireless interface of Intel AMT. For more information, see Disabling the Wireless Interface on page 227.

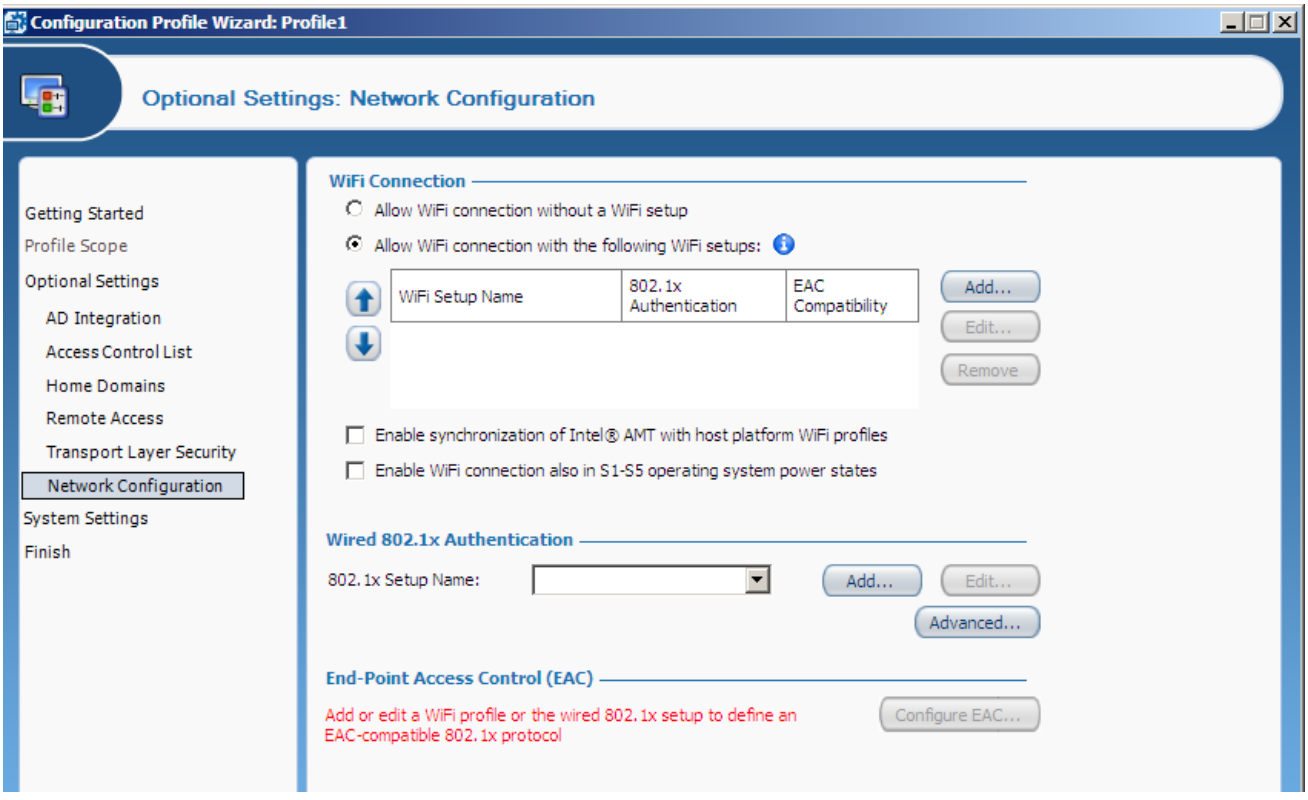


Figure 5-16: Network Configuration Window

To define network setups:

1. From the WiFi Connection section, select one of these:
   - **Allow WiFi connection without a WiFi setup** – Select this option if you want to allow 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** – Select this option if you want to define WiFi setups (see Creating WiFi Setups on the next page).

     After creating WiFi setups you can also do these tasks:
     - 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.

     Note:

     If you enable support for WiFi synchronization (step 2), it is not mandatory to define WiFi setups in the profile.
2. (Optional) Intel AMT 6.0 and higher includes a Wireless Profile Synchronization feature. This feature enables synchronization of the wireless profiles in the operating system 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, support for this feature is enabled. To use this feature to synchronize profiles, the Intel PROSet/Wireless Software must be installed on the operating system. For more information, refer to the documentation of the Intel PROSet/Wireless Software.
3. (Optional) By default, connection to the Intel AMT device via the WiFi connection is available only when the operating system is in the S0 power state. (Enabling WiFi connection in all power states uses more battery power.) If you want to enable the WiFi connection in all S0-S5 power states, select **Enable WiFi connection also in S1-S5 operating system power states**.
4. If required, from the 802.1x Setup Name drop-down list, select the 802.1x setup to use on a wired LAN. This setup will be used 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 114).

5. (Optional) Define advanced wired 802.1x authentication options:

   a. Click **Advanced**. The Advanced Wired 802.1x Settings window opens.

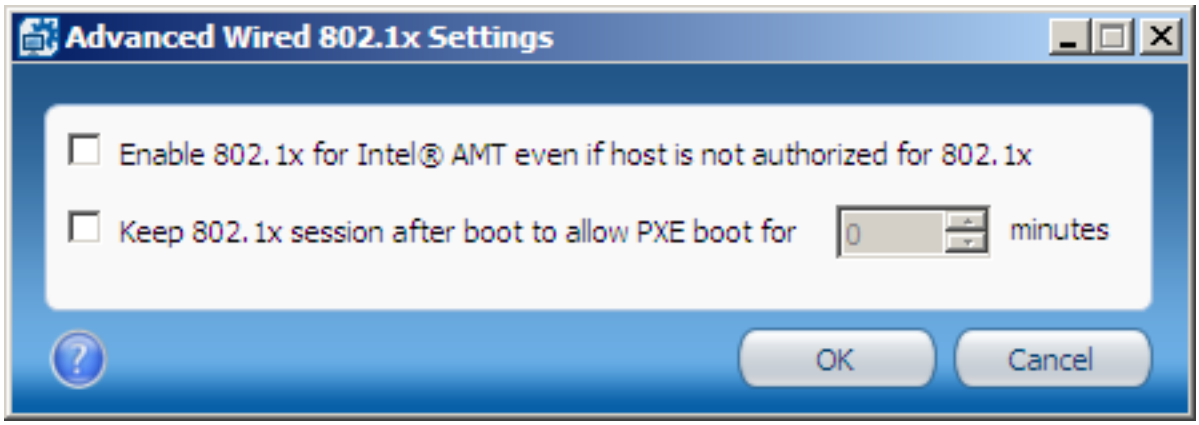


   Figure 5-17: Advanced Wired 802.1x Settings Window

   b. Select the check boxes of the options you want to enable:

   - **Enable 802.1x for Intel® 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 remains active 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 reset to zero.

   c. Click **OK**. The Advanced Wired 802.1x Settings window closes and the settings are saved.

6. If required, define the End-Point Access Control (EAC) parameters (see Defining End-Point Access Control on page 117).

5.11.1 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. The total number of WiFi setups (including 802.1x Wi-Fi setups) that can be configured depends on the version of Intel AMT:

- **Intel AMT 8.x and lower** – Up to a maximum of 15
- **Intel AMT 9.0 and higher** – Up to a maximum of 7

To create a WiFi setup:

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

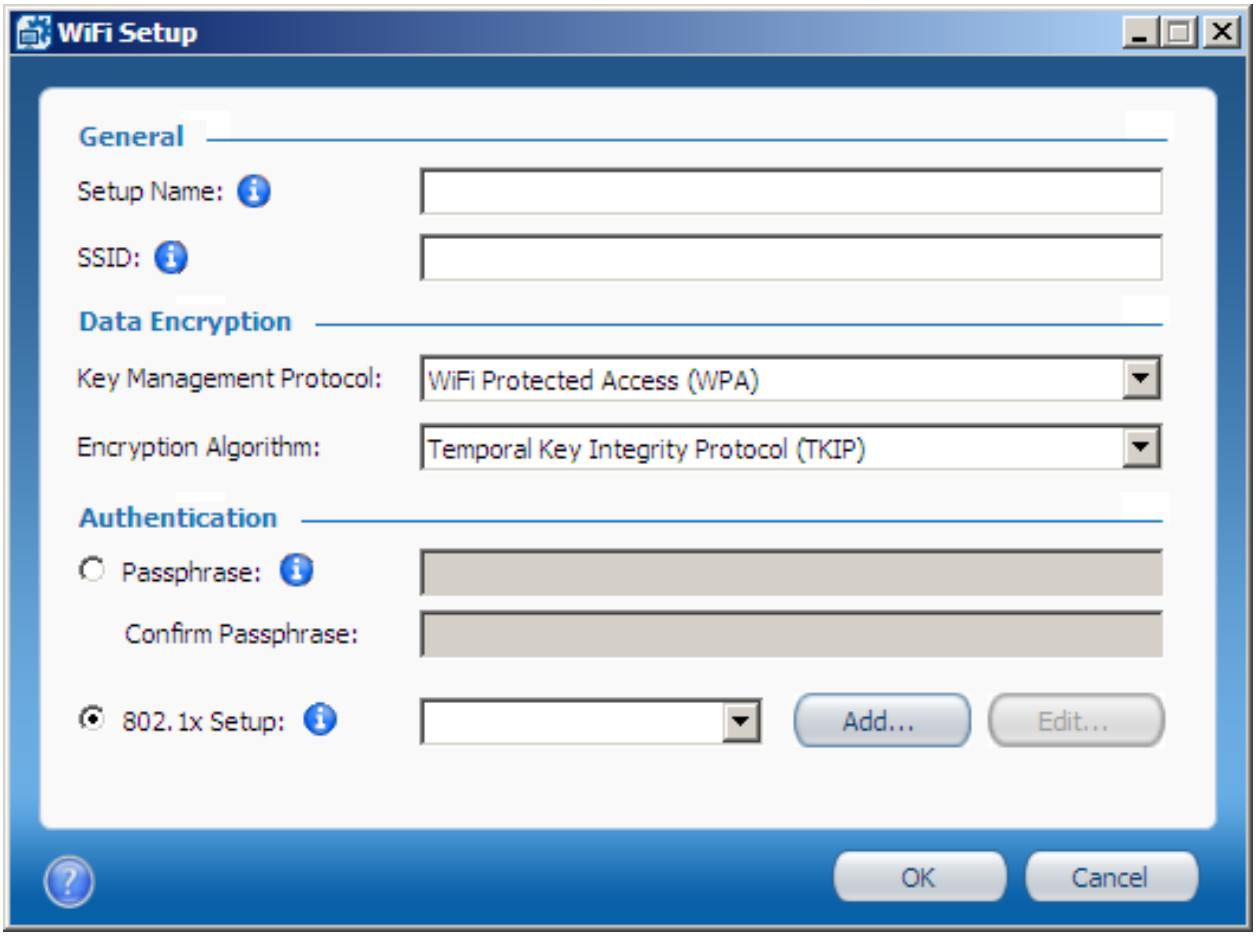


Figure 5-18: WiFi Setup Window

2. In the Setup Name field, enter a name for the WiFi setup. The setup name can be up to 32 characters, and must not contain (/ \ < > : ; * | ? ") characters.
3. In the SSID field, enter the Service Set Identifier (up to 32 characters) that identifies the specific WiFi network.
4. From the Key Management Protocol drop-down list, select one of these:
   - **WiFi Protected Access (WPA)**
   - **Robust Security Network (RSN)**
5. From the Encryption Algorithm drop-down list, select one of these:
   - **Temporal Key Integrity Protocol (TKIP)**
   - **Counter mode CBC MAC Protocol (CCMP)**
6. In the Authentication section, select one of these:
   - **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 the next page).
7. Click **OK**. The WiFi setup window closes and the setup is added to the list.

5.11.2 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:

802.1x setups require integration with Active Directory (see Defining Active Directory Integration on page 92) 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 opens.

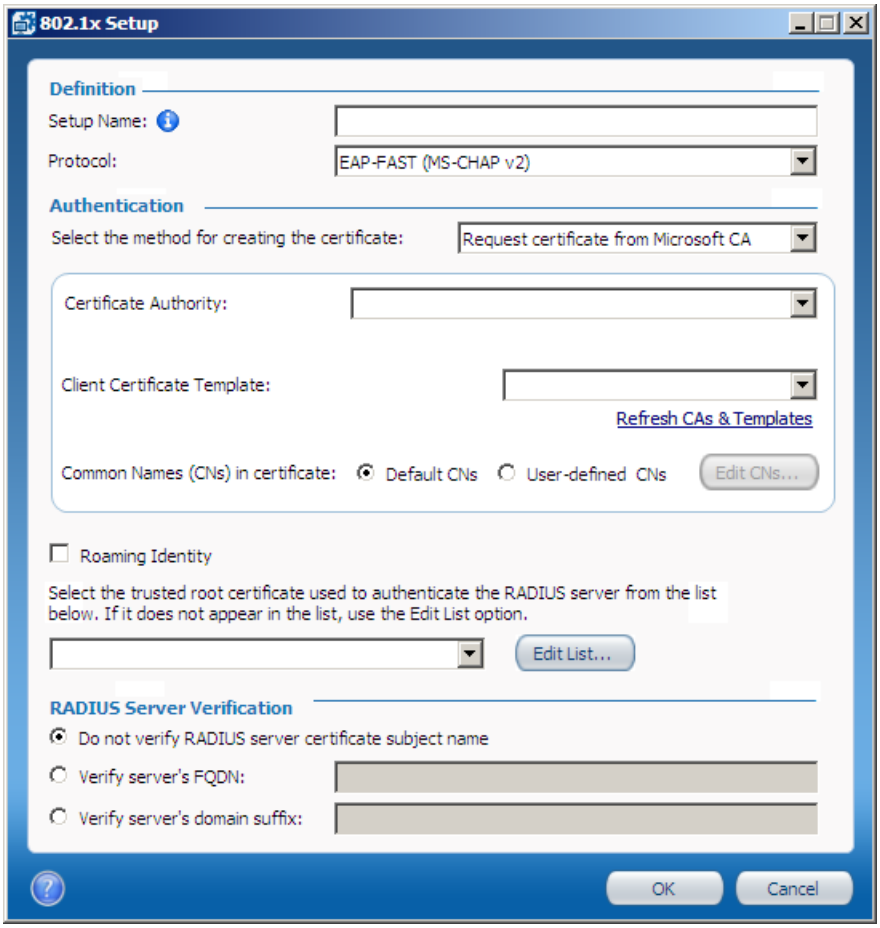


Figure 5-19: 802.1x Setup Window

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 the required protocol. The options in the Authentication section are enabled/disabled according to the protocol selected, as described in this table.

   Table 5-2: Authentication Options Per Protocol

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

4. From the Select the method for creating the certificate drop-down list, select the source for the certificate that will be installed in the Intel AMT device:
   - **Request certificate from Microsoft CA** – If you are using a Microsoft CA, continue from step 5.
   - **Request Certificate via CA plugin** – This option is only available if you have installed the optional CA plugin. For information about this option, see Using Intel SCS with the CA Plugin on page 204. If you select this option, enter the necessary settings (as defined by the plugin provider) and continue from step 6.
   - **Do not use a certificate** – Instead of using a certificate, authentication is done with a username and password. (This option is shown only if client certificates are optional for the Protocol selected in step 3.) Continue from step 6.

5. If the certificate will be requested from a Microsoft CA, do these steps:

   a. From the Certificate Authority drop-down list, select the Enterprise CA that Intel SCS will use to request a certificate that the RADIUS server can authenticate.

   b. From the Client Certificate Template drop-down list, select the template that will be used to create the client certificate. The templates shown are templates where the Subject Name is supplied in the request and the usage is "Client Authentication". For information how to create a template, see Defining Enterprise CA Templates on page 192.

   c. Define the Common Names that will be included in the Subject Name of the generated certificate. For more information, see Defining Common Names in the Certificate on page 205.

   Note:

   - To use this option, Intel SCS must have access to the CA during configuration (see Required Permissions on the CA on page 200).
   - If you are creating the profile on a computer that does not have access to the CA, the drop-down lists will not display the CA or the templates. If necessary, you can manually supply the CA name (in the format FQDN\CA Name) and the name of the template.

6. (Optional) To enable roaming, select the **Roaming Identity** check box. The user will connect to the RADIUS server with an identity of Anonymous.
7. If a trusted root certificate is required (see the table in step 3), select it from the list of trusted root certificates. If it does not appear in the list, click Edit List to define the location of the trusted root certificate (see Defining Trusted Root or Intermediate Certificates (CAs) on page 104). This certificate will be used in the 802.1x setup to authenticate with a RADIUS server.
8. From the RADIUS Server Verification section, select one of these:
   - **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.
9. Click **OK**. The 802.1x Setup window closes and the 802.1x setup is saved.

5.11.3 Defining End-Point Access Control

If the 802.1x profile's protocol supports End-Point Access Control (EAC), you can use NAC/NAP authentication along with the RADIUS server to authenticate the Intel AMT device.

> **Note:**
>
> EAC requires integration with Active Directory (see Defining Active Directory Integration on page 92) and an Enterprise-root CA.

To define EAC:

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

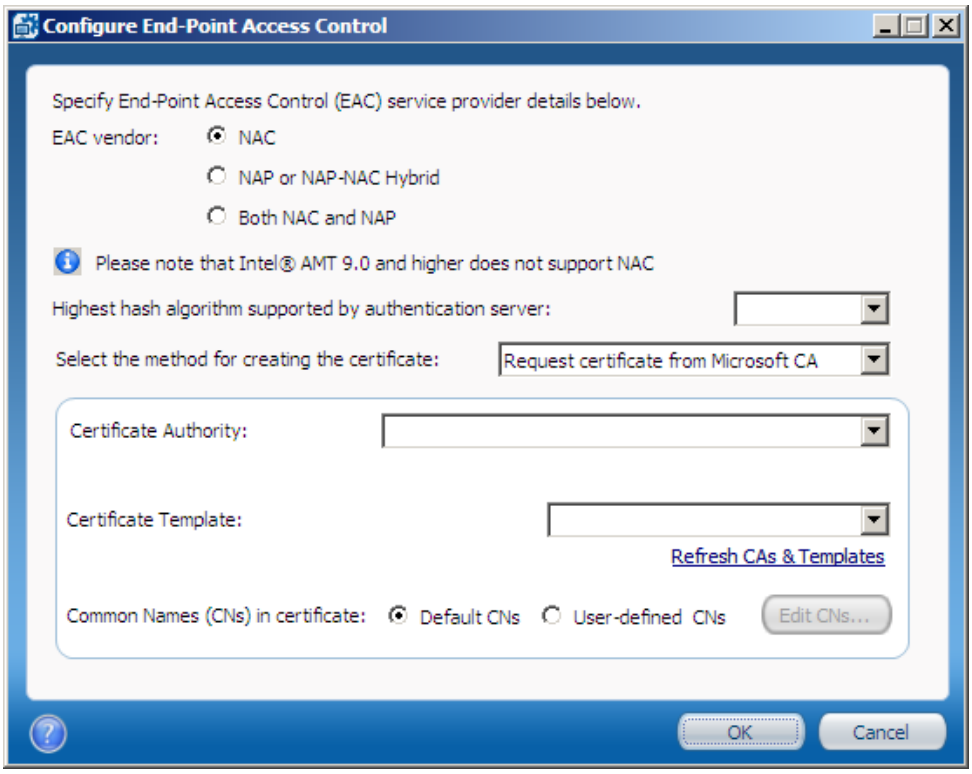


Figure 5-20: Configure End-Point Access Control Window

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

   Note:

   Intel AMT 9.0 and higher does not support NAC. This means that if you select the NAC option, EAC will not be configured on systems with Intel AMT 9.0 and higher configured using this profile.

3. From the Highest hash algorithm supported by the authentication server drop-down list, select one of these:
   - SHA-1
   - SHA-256 (only supported on Intel AMT 6.0 and higher)
   - SHA-384 (only supported on Intel AMT 6.0 and higher)
4. From the Select the method for creating the certificate drop-down list, select the source for the certificate that will be installed in the Intel AMT device:
   - **Request certificate from Microsoft CA** – By default, the settings for this option are displayed. If you are using a Microsoft CA, continue from step 5.
   - **Request Certificate via CA plugin** – This option is only available if you have installed the optional CA plugin. For information about this option, see Using Intel SCS with the CA Plugin on page 204. If you select this option, enter the necessary settings (as defined by the plugin provider) and continue from step 6.
5. If the certificate will be requested from a Microsoft CA, do these steps:

   a. From the Certificate Authority drop-down list, select the Enterprise CA that Intel SCS will use to request a certificate for EAC posture signing.

   b. From the Certificate Template drop-down list, select the template that will be used to create the client certificate. The templates shown are templates where the Subject Name is supplied in the request. For information how to create a template, see Defining Enterprise CA Templates on page 192.

   c. Define the Common Names that will be included in the Subject Name of the generated certificate. For more information, see Defining Common Names in the Certificate on page 205.

   Note:

   - To use this option, Intel SCS must have access to the CA during configuration (see Required Permissions on the CA on page 200).
   - If you are creating the profile on a computer that does not have access to the CA, the drop-down lists will not display the CA or the templates. If necessary, you can manually supply the CA name (in the format FQDN\CA Name) and the name of the template.

6. Click **OK**. The Configure End-Point Access Control window closes.

5.12 Defining System Settings

The System Settings window of the Configuration Profile Wizard lets you define several settings in the Intel AMT device.

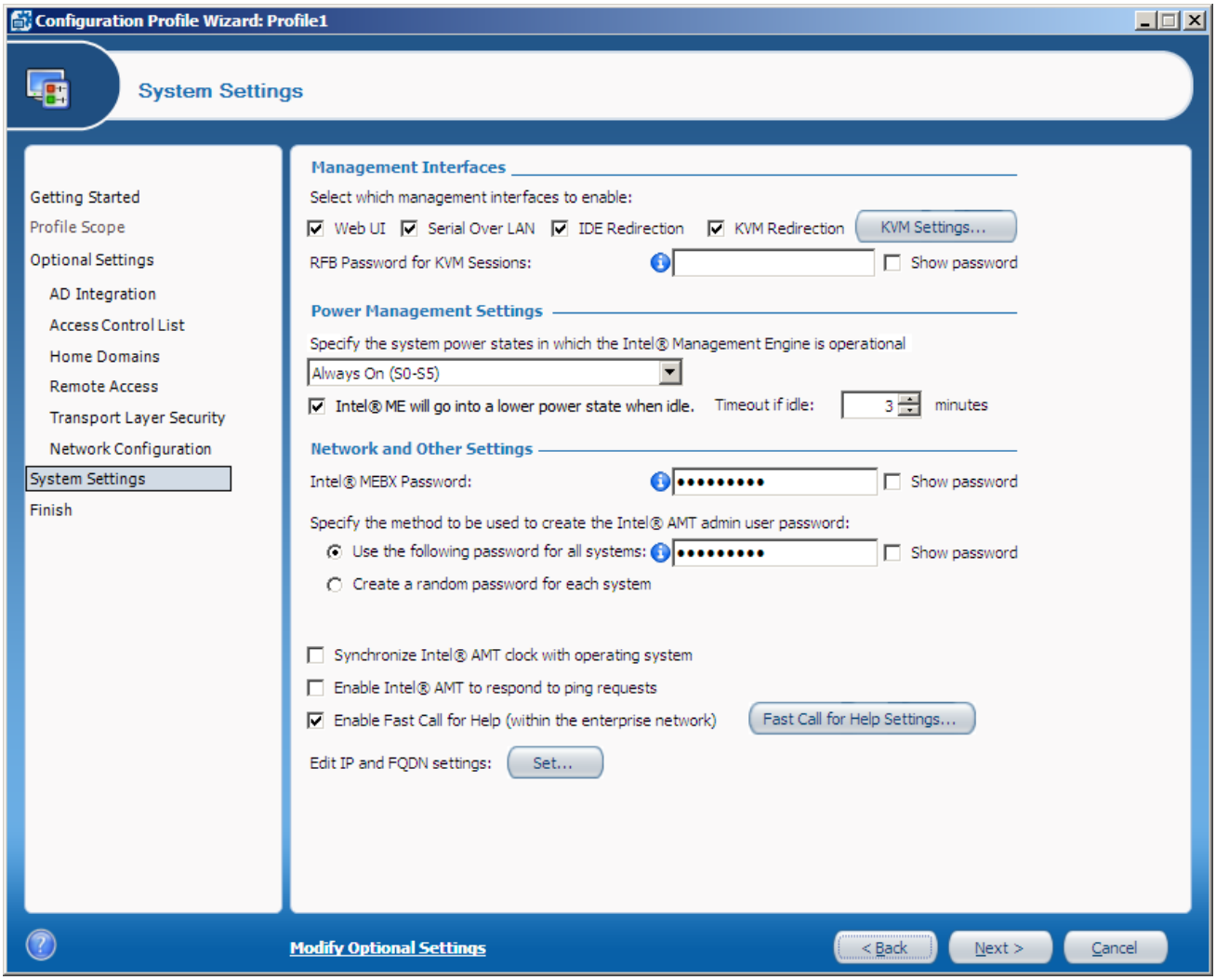


Figure 5-21: System Settings Window

For information about these settings, see:

- Management Interfaces on the next page
- Power Management Settings on page 121
- Network and Other Settings on page 121

Management Interfaces

1. Select the interfaces you want to open on the Intel AMT system:
   - **Web UI** – Enables you to manage and maintain Intel AMT systems using a browser-based interface.
   - **Serial Over LAN** – 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. Available through AMT 10
   - **USB Redirection** – USB-R enables you to map a drive on the Intel AMT system to a remote image or drive. In contrast to IDE-R, which presents remote floppy or CD drives as though they were integrated in the host machine, USB-R presents remote drives as though they were connected via a USB port. Available on AMT 11.0 and higher
   - **KVM Redirection** – Opens the KVM Redirection interface. For more information about KVM, see Support for KVM Redirection on page 24.
2. (Optional) When the KVM Redirection check box is selected, the RFB Password for KVM Sessions field is enabled. This password is only necessary if your VNC client uses port 5900 (see VNC Clients on page 24). If you enter a password, it must be EXACTLY eight characters (see Password Format on page 11).
3. (Optional) By default, user consent is necessary before a KVM redirection session can begin (see User Consent on page 16). If you want to change the user consent settings for KVM redirection sessions:
   a. Click **KVM Settings**. The KVM Redirection Settings window opens.

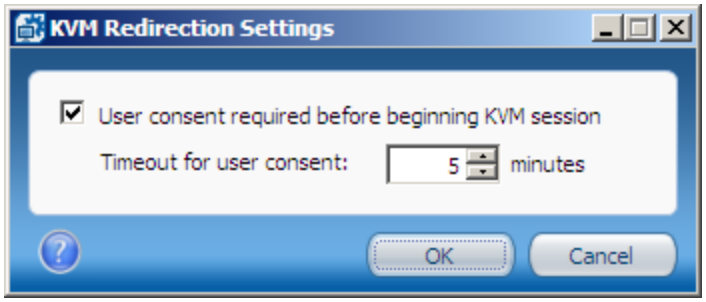


Figure 5-22: KVM Redirection Settings Window

   b. If you want to remove the user consent requirement, clear the **User consent required before beginning KVM session** check box.

> **Note:**
>
> User consent is mandatory for Intel AMT 6.2 and higher devices if they are configured in Client Control mode. Thus, if you want to remove the user consent requirement, you must configure these devices in Admin Control mode.

   c. If User Consent is required, the Timeout for user consent field defines 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.

Power Management Settings

1. From the drop-down list, select one of these:
   - **Always On (S0-S5)** – If the system is connected to the power supply, the Intel AMT manageability features are available in any of the system power states. This is the recommended setting.
   - **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. You cannot select this setting if the Enable WiFi connection also in S1-S5 operating system power states check box is selected (in the Network Configuration window).
2. (Optional) If you selected Always on (S0-S5), you can select the **Intel® ME will go into a lower power state when idle** check box. If the Intel AMT device supports this feature, the device will go to sleep when there is no activity. When a request arrives, the device automatically wakes up. The Time out if idle field defines the number of minutes the device must wait before it can go to sleep.

Network and Other Settings

1. In the Intel® MEBX Password field, enter a password for the Intel MEBX (see Password Format on page 11). If the RCS detects that the current password in the Intel MEBX is the default password, it will replace it with this password. If the default Intel MEBX password was already replaced, this password is ignored (it is not set in the Intel MEBX).

   Note:

   If the Intel AMT system will be put in the Client Control mode, this password will not be set in the Intel MEBX. For more information, see Access to the Intel MEBX on page 18.

2. Define the password of the default admin user built into each Intel AMT device:
   - **Use the following password for all systems** – The password you define here (see Password Format on page 11) is set in all devices configured with this profile.
   - **Create a random password for each system**– A different (random) password is generated for each device.
   - **Use a Master Password to create a password for each system** – This option is only shown if a Digest Master Password is set in the RCS.

   Note:

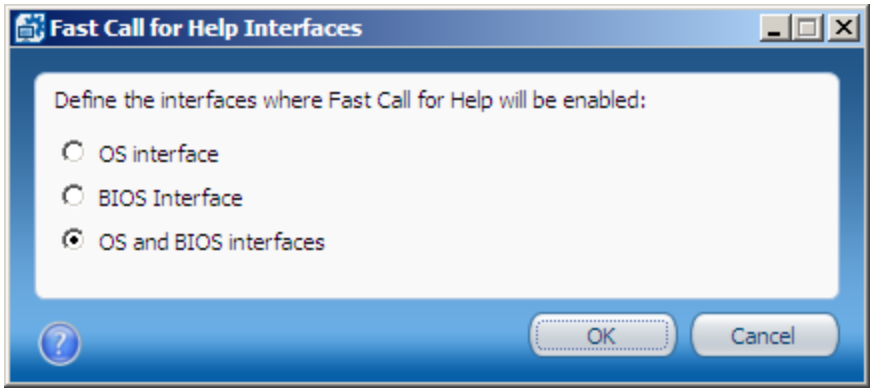
   For important information about these password options (see Admin Permissions in the Intel AMT Device on page 18).

3. (Optional) Select **Synchronize Intel® AMT clock with the operating system**. When this check box is selected, the Intel AMT clock will automatically synchronize with the operating system clock. This option is available only from Intel AMT 9.0 and higher.

   Note:

   This option can make it possible for attackers (via a compromised operating system) to change the Intel AMT clock. An unsynchronized clock can cause Kerberos based authentication to Intel AMT to fail. Select this option only if you are sure that the operating systems in your organization are sufficiently secured.

4. (Optional) **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 respond.
5. (Optional) You can define which interfaces are open for the local Fast Call for Help feature. If the computer is inside the enterprise network, the user can initiate a connection request to connect to a management console. By default, the user can access this option from the operating system and from the BIOS. To change this setting, do one of these:
   - To close both interfaces, clear the **Enable Fast Call for Help (within the enterprise network)** check box.
   - To select which interface to open, click **Fast Call For Help Settings** and select the interface from the Fast Call for Help interfaces window:



   Note:

   - You cannot make changes to this setting if a Fast Call For Help trigger was defined in a Remote Access policy. The setting in the policy will be used for remote and local connection requests.
   - To enable the Fast Call for Help feature from outside the enterprise network, see Defining Remote Access on page 100.

6. (Optional) Click **Set** to define the source that Intel SCS will use to define the IP and FQDN of the Intel AMT device. This step is only required if you need to change the default settings (see Defining IP and FQDN Settings below).

> **Note:**
>
> The default network settings that Intel SCS puts in the device will operate correctly for most network environments.

5.12.1 Defining IP and FQDN Settings

Each Intel AMT device can have its own IP and FQDN settings. The IP and FQDN settings are usually the same as those defined in the host operating system, but they can be different. Intel SCS puts these settings into the Intel AMT device.

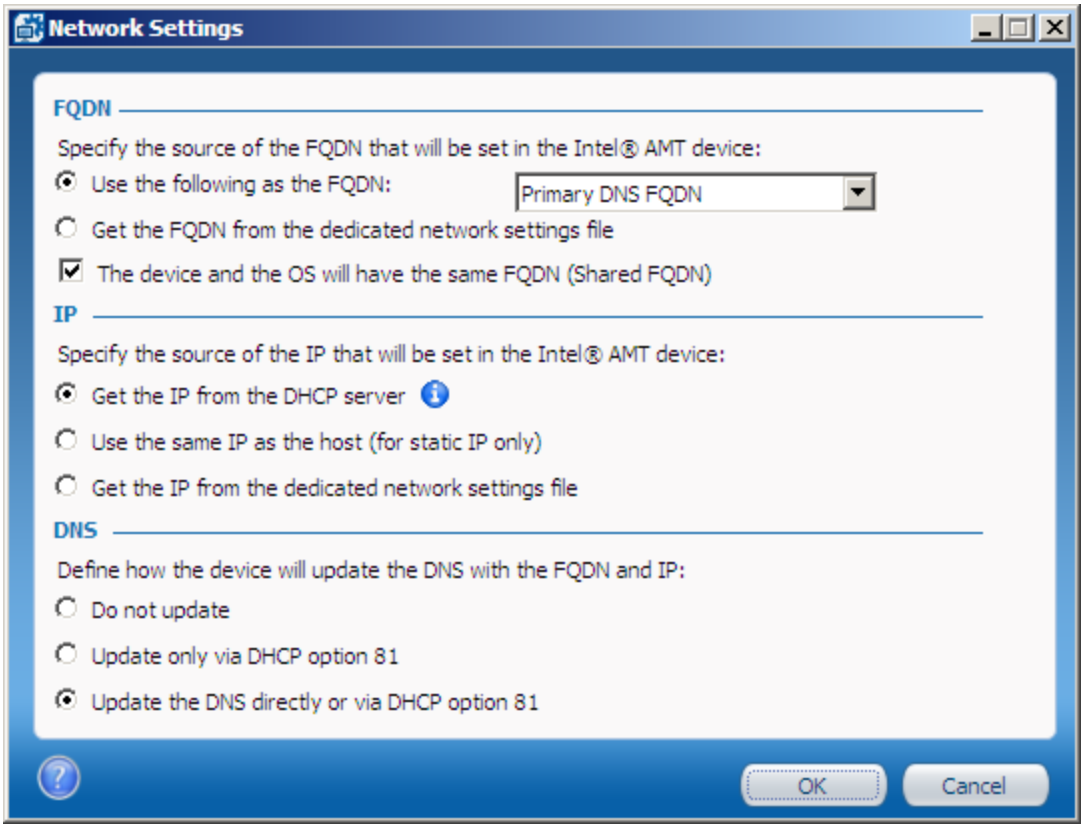


Figure 5-23: Network Settings Window

To define the IP and FQDN settings:

1. From the FQDN section, select the source for the FQDN (hostname.suffix):
   - **Use the following as the FQDN**:
     - **Primary DNS FQDN** – The hostname part of the FQDN is the hostname from the host operating system. The suffix is the "Primary DNS Suffix" from the host operating system. This is the default setting and is correct for most network environments.
     - **On-board LAN connection-specific DNS FQDN** – The hostname part of the FQDN is the hostname from the host operating system. The suffix is the "Connection-specific DNS Suffix" of the on-board wired LAN interface.
     - **Host Name** – Takes the host name from the operating system. The suffix is blank.
     - **Active Directory FQDN** – The hostname part of the FQDN is the hostname from the host operating system. The suffix is the AD domain of which the host operating system is a member.
     - **DNS Look Up FQDN** – Takes the name returned by an "nslookup" on the IP address of the on-board wired LAN interface. To use this option, the DNS must be configured correctly with Reverse Lookup Zones.
   - **Get the FQDN from the dedicated network settings file**

     Note:

     If you select a dedicated network settings file as the source for the FQDN or IP:
     - Make sure that the file contains only the settings (FQDN / IP) that you want to supply using the file. For information about the format and tags of the XML file, see the `NetworkSettings.xml` example file located in the `sample_files` folder.
     - Do not forget to supply the path to the file using the `/NetworkSettingsFile` parameter of the Configurator CLI command.
2. (Optional) Intel AMT 6.0 and higher includes a setting called "Shared FQDN". This setting can change the behavior of the Intel AMT device when using option 81 of the DHCP server to update DNS:
   - When this setting is true, the Intel AMT device will send broadcast queries only when the operating system is not running. This is the default behavior of all Intel AMT versions that do not support the Shared FQDN setting.
   - When false, the device will always send its own broadcast queries, even when the operating system is running. For Intel AMT 6.0 and higher devices that will be configured with a dedicated FQDN, clear this check box: **The device and the OS will have the same FQDN (Shared FQDN)**.
3. From the IP section, select the source for the IP settings:
   - **Get the IP from the DHCP server**
   - **Use the same IP as the host (for static IP only)**
   - **Get the IP from the dedicated network settings file**

4. In the DNS section, define how Intel AMT 6.0 and higher will update the Domain Name System (DNS) with the FQDN and IP:
   - **Do not update** – Disables all DNS updates by the Intel AMT device.
   - **Update only via DHCP option 81** – The device will use the DHCP option 81 to request that the DHCP server update the DNS on its behalf. On Intel AMT 6.x and 7.x systems, Intel SCS only supports this option on the latest firmware versions.
   - **Update the DNS directly or via DHCP option 81** – Intel AMT 6.0 and higher includes the Intel AMT Dynamic DNS Update (DDNS Update) Client. When enabled, this client can periodically update the DNS with the FQDN and IP address configured in the Intel AMT device. When selected, the device uses option 81 to ask the DHCP for permission to update the DNS. Intel AMT will send DDNS updates based on the policy configured in the DHCP server returned in the DHCP option 81 flags.

   Note:

   All systems that have Intel AMT 5.x or lower are always configured to update the DNS via DHCP option 81. (This is the only option that those versions support.)

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

Chapter 6

Using the Configurator

This chapter describes how to use the Configurator.

For more information, see:

6.1 About the Configurator

The Command Line Interface (CLI) of the Configurator component lets you automatically do tasks on multiple Intel AMT systems. The Configurator is run locally on the Intel AMT system using a script or a batch file. If possible, the Configurator does the necessary task locally on the system. If not, the Configurator sends the task to the RCS. The CLI also includes commands that make the Configurator send the task to the RCS, even if it can be done locally.

To install the Configurator, run the file `ACUConfigInstaller.msi`, which is is located in the Configurator folder.

Once installed, the Configurator (`ACUConfig.exe`) resides in the installation folder. The default installation path for `ACUConfig.exe` is "`C:\Program Files (x86)\Intel\SCS ACUConfig`".

Note

Intel recommends following security best practices, including installing the Configurator in the suggested, default location. The default file path is "`C:\Program files (x86)\Intel\SCS ACUConfig`". Otherwise, be sure to install and run ACUConfig.exe in a system-privileged folder on the target system.

6.2 CLI Syntax

The Configurator CLI is not case-sensitive. To view a list of the available CLI commands, type `ACUConfig` (with no parameters) and press <Enter>.

This is the general syntax:

`ACUConfig.exe [global options]` command [command arguments and options]

To view syntax of a specific command, type the command name followed by "/?".

These conventions are used in the command syntax of the examples:

- Optional parameters are enclosed in square brackets [ ]
- User-defined variables are enclosed in angled brackets < >
- Mutually exclusive parameters are separated with a pipe |
- Where necessary, braces { } are used to group elements together to eliminate ambiguity in the syntax.

6.3 Configurator Log Files

The Configurator records errors and other log messages in two locations:

- In the Windows Event Viewer Application log of the Intel AMT system.
- In a log file. By default:
  - A new log file is created each time you run the Configurator. You can use the `/KeepLogFile` global option to change this default.
  - The log file is saved in the folder where the Configurator is located, and has this format:

    `ACUlog_HostName_YYYY-MM-DD-HH-MI-SS.Log`

    For example: `ACUlog_ComputerX_2013-05-01-11-05-57.log`.

    You can use the `/Output` File global option to change the default name and location of the log file.

6.4 CLI Global Options

You can use any of these global options with the CLI commands:

- `/LowSecurity` – Disables authentication of the `ACU.dll` digital signature. For more information, see Digital Signing of Files on page 12.
- `/Verbose` – Creates a detailed log
- `/KeepLogFile` – Appends the current log to the existing log file
- `/Output {Console | File <logfile> | Silent}` – Defines where errors and other log messages will be recorded:
  - `Console` – Shows log messages only on the Console screen
  - `File <logfile>` – Lets you change the default name and location of the log file. Supply the full path and name for the log file in the `<logfile>` parameter.
  - `Silent` – Do not record any log messages (Console or log file)

Note

To save log messages to a file and also display them on the Console screen, use the `/Output` parameter twice. For example: `/Output File <logfile> /Output Console`.

6.5 Admin Password Parameter Errors

If the parameter `AdminPassword <password>` is used to provide the current password of the default Digest admin user defined in the Intel AMT device, and the `<password>` value does specified does not meet the required password format described in Password Format on page 11, then ACUConfig will return an error due to the unmet password requirements. However, if the password is "admin", then ACUConfig will not return an error, although this specific password is ignored (is not provided to the Intel AMT device).

6.6 Verifying the Status of Intel AMT

Command	`Status`
Description	Provides details about the status of Intel AMT
Syntax	`ACUConfig.exe [global options] Status`
Parameters	
`[global options]`	See CLI Global Options on the previous page

6.7 Discovering Systems

Command	`SystemDiscovery`
Description	Gets data about the Intel AMT device and the host platform. The data can be saved in an XML file on the system and/or in the registry. You can also send the data to the database via the RCS (in database mode). If saved in the registry, the data is saved in each system at this location: • 32-bit and 64-bit operating systems: `HKLM\SOFTWARE\Intel\Setup and Configuration Software\SystemDiscovery` • In addition, on 64-bit operating systems: `HKLM\SOFTWARE\Wow6432Node\Intel\Setup and Configuration Software\SystemDiscovery` This command is just one of the discovery options included with Intel SCS. For more information, see What are the Discovery Options? on page 3. **Note:** • On systems that do not have Intel AMT, this command gets data from the host platform only.
Syntax	`ACUConfig.exe [global options] SystemDiscovery {[<filename>] | [/NoFile]} [/NoRegistry] [/ReportToRCS] [/AdminPassword <password>] [/RCSaddress <RCSaddress>] {[/WMIUser <username>] [/WMIUserPassword <password>]} [/SourceForAMTName <source>] [/NetworkSettingsFile <file>] [/RCSBusyRetryCount <retries>]`
Parameters	
`[global options]`	See CLI Global Options on the previous page

<filename>	By default, the name of the XML file is the FQDN of the system and it is saved in the same folder as the Configurator. The default installation path of the Configurator is "C:\Program Files (x86)\Intel\SCS ACUConfig". You can change this default name and location by supplying the <filename> parameter. **Example:** ACUConfig.exe SystemDiscovery C:\MyXMLFile.xml This example creates an XML file named "MyXMLFile" in the root of C. In addition, a log file is created (see Configurator Log Files on page 127).
/NoFile	Do not save data in an XML file. If you use this parameter, do not use the <filename> parameter.
/NoRegistry	Do not save data in the registry of the system
/ReportToRCS	Sends the data to the RCS. You can only use this parameter if the RCS is installed in database mode. If this parameter is supplied, the data is updated in the database record of the system. If this parameter is supplied, the /RCSAddress parameter is mandatory. **Note:** This parameter is used as part of the process to fix Host FQDN mismatches. For more information, see Detecting and Fixing Host FQDN Mismatches on page 172.
/AdminPassword <password>	The current password of the default Digest admin user defined in the Intel AMT device. The SystemDiscovery command gets some of the data about Intel AMT using the WS-Man interface. To use this interface, administrator permissions in Intel AMT are necessary. Without administrator permissions, this data cannot be retrieved and a warning message will be recorded in the log. This parameter is NOT necessary if any of these are true: • The device is in an unconfigured state • The user account running the Configurator is a Kerberos account that is configured in the Intel AMT device with administrator permissions • You supply the /RCSAddress parameter and the RCS can find the password in the database, in a profile, or using the Digest Master Password. See Admin Password Parameter Errors on page 128 for information on errors resulting from this parameter.
/RCSaddress <RCSaddress>	The IP or FQDN of the computer running the RCS
/WMIUser <username>	The name (in the format domain\username) of a user with WMI permissions on the computer running the RCS. This parameter is only required if you run the Configurator with a user account that does not have WMI permissions on the RCS computer. (But only if you want to connect to the RCS.)

/WMIUserPassword <password>	The password of the WMI user
/SourceForAMTName <source>	Defines how the FQDN (hostname.suffix) for the Intel AMT device is constructed. Valid values: • DNS — The hostname part of the FQDN is the hostname from the host operating system. The suffix is the "Primary DNS Suffix" from the host operating system. This is the default setting, and is correct for most network environments. • SpecificDNS — The hostname part of the FQDN is the hostname from the host operating system. The suffix is the "Connection-specific DNS Suffix" of the on-board wired LAN interface. • AD — The hostname part of the FQDN is the hostname from the host operating system. The suffix is the AD domain of which the host operating system is a member. • DNSLOOKUP — Takes the FQDN returned by an "nslookup" on the IP address of the on-board wired LAN interface. To use this option, the DNS must be configured correctly with Reverse Lookup Zones. • HOST — Takes the hostname from the host operating system. The suffix is blank. **Note:** When this parameter is not supplied, the default source for the FQDN is "DNS". However, if the /NetworkSettingsFile parameter is supplied (and FQDN data is included in the file), the FQDN is taken from the file.
/NetworkSettingsFile <file>	This parameter tells the Configurator to get the IP and/or the FQDN from a dedicated network settings file. For information about the required XML format, see the NetworkSettings.xml example file located in the sample_files folder.
/RCSBusyRetryCount <retries>	Defines the number of times to resend the request to the RCS if the RCS returns a status of busy. The maximum number of retries is 100. Each request is sent after a random period of time. If not supplied, the default for this parameter is 0.

6.8 Configuring Systems (Unified Configuration)

Command	`ConfigAMT`
Description	Configures Intel AMT with settings in a configuration profile (XML file). Configured systems are reconfigured. You can use this command with the unified configuration process. If the Intel AMT device supports host-based configuration, the configuration is done locally. If not, configuration is done remotely by the RCS. For more information, see Unified Configuration Process on page 9. **Note:** If you run `ConfigAMT` on a new system locally (in the host-based configuration), the Intel® Management Engine BIOS Extension (MEBX) password will not be reset from the default password, "admin," while the system is in admin control mode. Therefore, you must run `ConfigViaRCSOnly` after running `ConfigAMT` locally, to set the MEBX password. See Configuring Systems using the RCS on page 134.
Syntax	`ACUConfig.exe [global options] ConfigAMT <filename> [/DecryptionPassword <password>] [/AbortOnFailure] [/AdminPassword <password>] [/LongRandomPassword] [/ADOU <ADOU path>][/NetworkSettingsFile <file>] {[/FileToRun <filename>] [/FileHash <SHA256 hash>] [/FileUser <username>] [/FilePassword <password>]}`
Parameters	
`[global options]`	See CLI Global Options on page 128
`<filename>`	The XML file containing the configuration parameters for this Intel AMT system
`/DecryptionPassword <password>`	Mandatory if any of the files that the Configurator will use are encrypted (see File Encryption on page 11)
`/AbortOnFailure`	If configuration fails, put the Intel AMT device in the "Not Provisioned" mode. This parameter is applicable only for systems that were unconfigured when the command started (during reconfiguration this parameter is ignored). **Warning:** A full unconfiguration will occur and as a result, any certificate hashes and PKI DNS suffix manually entered into the MEBX will be deleted.

/AdminPassword <password>	The current password of the default Digest admin user defined in the Intel AMT device. This parameter is NOT necessary if any of these are true: • The device is in an unconfigured state • Intel SCS can find the Digest admin password (in one of the profiles or using a Digest Master Password) • The user account running the Configurator/RCS is a Kerberos account that is configured in the Intel AMT device with administrator permissions See Admin Password Parameter Errors on page 128 for information on errors resulting from this parameter.
/LongRandomPassword	The /LongRandomPassword is used by the ACUConfig.exe as a flag so that ACUConfig will ignore the password set in the profile and instead generate a random long (32 char) password and set it as the admin password for that platform. If the user wants to know what password was set, then he must use the /filetorun tag in order to run a script, the seventh "%7" parameter of this script will be the password that was generated by the acuconfig.exe. It is recommended that this flag only be used alongside the /filetorun flag, and for the script to execute a report to RCS command so that this password gets stored in the database. Otherwise the user will not know what password was used and his platform won't unconfigure.
/ADOU <ADOU path>	The path to the Active Directory Organizational Unit (ADOU) containing the AD object of configured systems. If this parameter is supplied, the Configurator will delete the existing AD object representing the system. A new AD object is created in the ADOU defined in the configuration profile.
/NetworkSettingsFile <file>	The path to a file that contains the network settings (FQDN and/or IP) to put in the Intel AMT device. Only use this parameter if you defined the source for at least one of these settings as a dedicated network settings file. For more information, see Defining IP and FQDN Settings on page 123.
/FileToRun /FileHash /FileUser /FilePassword	The Configurator can use these parameters to run a script after the command has completed successfully. For more information, see Scripts Run by the Configurator on page 150.

6.9 Configuring Systems using the RCS

Command	`ConfigViaRCSOnly`
Description	Sends a configuration request to the RCS. The RCS remotely configures Intel AMT using a profile located in the RCS. Configured systems are reconfigured. The RCS uses one of the TLS protocols (PSK or PKI) during the configuration process (see Security Before and During Configuration on page 17). **Note:** This command puts the Intel AMT device in the Admin Control mode (see Control Modes on page 15).
Syntax	`ACUConfig.exe [global options] ConfigViaRCSOnly <RCSaddress> <profilename> [/AbortOnFailure] [/AdminPassword <password>] {[/WMIUser <username>] [/WMIUserPassword <password>]} [/ADOU <ADOU path>] [/NetworkSettingsFile <file>] [/RCSBusyRetryCount <retries>]`
Parameters	
`[global options]`	See CLI Global Options on page 128
`<RCSaddress>`	The IP or FQDN of the computer running the RCS
`<profilename>`	The profile in the RCS containing the configuration parameters
`/AbortOnFailure`	If configuration fails, put the Intel AMT device in the "Not Provisioned" mode. This parameter is applicable only for systems that were unconfigured when the command started (during reconfiguration this parameter is ignored).
`/AdminPassword <password>`	The current password of the default Digest admin user defined in the Intel AMT device. This parameter is NOT necessary if any of these are true: • The device is in an unconfigured state • Intel SCS can find the Digest admin password (in one of the profiles or using a Digest Master Password) • The user account running the RCS is a Kerberos account that is configured in the Intel AMT device with administrator permissions See Admin Password Parameter Errors on page 128 for information on errors resulting from this parameter.
`/WMIUser <username>`	The name (in the format domain\username) of a user with WMI permissions on the computer running the RCS. This parameter is only required if you run the Configurator with a user account that does not have WMI permissions on the RCS computer.

/WMIUserPassword <password>	The password of the WMI user
/ADOU <ADOU path>	The path to the Active Directory Organizational Unit (ADOU) containing the AD object of configured systems. If this parameter is supplied, the RCS will delete the existing AD object representing the system. A new AD object is created in the ADOU defined in the configuration profile.
/NetworkSettingsFile <file>	The path to a file that contains the network settings (FQDN and/or IP) to put in the Intel AMT device. Only use this parameter if you defined the source for at least one of these settings as a dedicated network settings file. For more information, see Defining IP and FQDN Settings on page 123.
/RCSBusyRetryCount <retries>	Defines the number of times to resend the request to the RCS if the RCS returns a status of busy. The maximum number of retries is 100. Each request is sent after a random period of time. If not supplied, the default for this parameter is 0.

6.10 Adding a Configured System or Updating an Unconfigured System

Command	NotifyRCS
Description	Sends a request to the RCS to add a configured Intel AMT system to the database. The RCS then tries to connect to the Intel AMT device. If successful, the system is added to the database in the "Managed" state. If not, the system is added to the database in the "Unmanaged" state. Can also send a request to the RCS to update the configuration status of an unconfigured AMT system to "Unconfigured. To understand when this command is necessary, and the limitations of the Unmanaged state, see: • About Adding and Deleting Systems on page 161 • Changing the Managed State of Systems on page 171 **Note:** After running this command some information in the database record for the added system might be missing (for example, details about the configuration profile). To update this information, run the SystemDiscovery command (see Discovering Systems on page 129).
Syntax	ACUConfig.exe [global options] NotifyRCS <RCSaddress> [/AdminPassword <password>] {[/WMIUser <username>] [/WMIUserPassword <password>]} [/RCSBusyRetryCount <retries>]
Parameters	

[global options]	See CLI Global Options on page 128
<RCSaddress>	The IP or FQDN of the computer running the RCS
/AdminPassword <password>	The current password of the default Digest admin user defined in the Intel AMT device. After adding the system to the database, the RCS will try to connect to the system using the password. If you use this parameter, make sure that you supply the correct password. If the password is not correct, the RCS might not be able to connect to the system after it is added to the database. See Admin Password Parameter Errors on page 128 for more information on errors resulting from this parameter.
/WMIUser <username>	The name (in the format domain\username) of a user with WMI permissions on the computer running the RCS. This parameter is only required if you run the Configurator with a user account that does not have WMI permissions on the RCS computer.
/WMIUserPassword <password>	The password of the WMI user
/RCSBusyRetryCount <retries>	Defines the number of times to resend the request to the RCS if the RCS returns a status of busy. The maximum number of retries is 100. Each request is sent after a random period of time. If not supplied, the default for this parameter is 0.

6.11 Maintaining Configured Systems

Command	MaintainAMT
Description	Runs specific maintenance tasks on Intel AMT, based on settings in the <filename> XML file. If the Intel AMT device supports host-based configuration, the maintenance tasks are done locally. If not, the tasks are done remotely by the RCS.
Syntax	ACUConfig.exe [global options] MaintainAMT <filename> <task> [<task>...] [/DecryptionPassword <password>] [/AdminPassword <password>] [/NetworkSettingsFile <file>] {[/FileToRun <filename>] [/FileHash <SHA256 hash>] [/FileUser <username>] [/FilePassword <password>]}
Parameters	
[global options]	See CLI Global Options on page 128
<filename>	The XML file containing the original configuration settings that were used to configure Intel AMT. Settings in the XML file not related to the specified maintenance tasks are ignored.

<task>	Define at least one of these maintenance tasks: • SyncAMTTime – Synchronizes the clock of the Intel AMT device with the clock of the computer running the RCS. If the device supports host-based configuration, the clock is synchronized with the clock of the host. This task is performed automatically when any of the other tasks are performed. • SyncNetworkSettings – Synchronizes network settings of the Intel AMT device as defined in the <NetworkSettings> tag of the <filename> XML file (see Defining IP and FQDN Settings on page 123) • ReissueCertificates – Reissues the certificates stored in the Intel AMT device. If the device contains 802.1x certificates, the RenewADPassword task is automatically done as well. • RenewADPassword – Changes the password of the Active Directory object representing the Intel AMT system. • RenewAdminPassword – Changes the password of the default Digest admin user in the Intel AMT device according to the password setting defined in the profile. • AutoMaintain – Automatically does only the maintenance tasks (listed here) that are necessary for this Intel AMT system. For more information, see: • About Maintenance Tasks on page 21 • Manual/Automatic Maintenance using the CLI on page 22
/DecryptionPassword <password>	Mandatory if any of the files that the Configurator will use are encrypted (see File Encryption on page 11)
/AdminPassword <password>	The current password of the default Digest admin user defined in the Intel AMT device. This parameter is NOT necessary if any of these are true: • Intel SCS can find the Digest admin password (in one of the RCS profiles or using a Digest Master Password) • The user account running the Configurator/RCS is a Kerberos account that is configured in the Intel AMT device with administrator permissions See Admin Password Parameter Errors on page 128 for information on errors resulting from this parameter.
/NetworkSettingsFile <file>	The path to a file that contains the network settings (FQDN and/or IP) to put in the Intel AMT device. Only use this parameter if you defined the source for at least one of these settings as a dedicated network settings file. For more information, see Defining IP and FQDN Settings on page 123.
/FileToRun /FileHash /FileUser /FilePassword	The Configurator can use these parameters to run a script after the command has completed successfully. For more information, see Scripts Run by the Configurator on page 150.

6.12 Maintaining Systems using the RCS

Command	`MaintainViaRCSOnly`
Description	Runs specific maintenance tasks on Intel AMT, based on settings in the `<profilename>`. All maintenance tasks are done remotely by the RCS.
Syntax	`ACUConfig.exe [global options] MaintainViaRCSOnly <RCSaddress> <profilename> <task> [<task>...] [/AdminPassword <password>] {[/WMIUser <username>] [/WMIUserPassword <password>]} [/NetworkSettingsFile <file>] [/RCSBusyRetryCount <retries>]`
Parameters	
`[global options]`	See CLI Global Options on page 128
`<RCSaddress>`	The IP or FQDN of the computer running the RCS
`<profilename>`	The profile in the RCS containing the original configuration settings that were used to configure Intel AMT. Settings in the profile not related to the specified maintenance tasks are ignored.

<task>	Define at least one of these maintenance tasks: • SyncAMTTime – Synchronizes the clock of the Intel AMT device with the clock of the computer running the RCS. This task is performed automatically when any of the other tasks are performed. • SyncNetworkSettings – Synchronizes network settings of the Intel AMT device as defined in the <NetworkSettings> tag of the <filename> XML file (see Defining IP and FQDN Settings on page 123) • ReissueCertificates – Reissues the certificates stored in the Intel AMT device. If the device contains 802.1x certificates, the RenewADPassword task is automatically done as well. • RenewADPassword – Changes the password of the Active Directory object representing the Intel AMT system. • RenewAdminPassword – Changes the password of the default Digest admin user in the Intel AMT device according to the password setting defined in the profile. • AutoMaintain – Automatically does only the maintenance tasks (listed here) that are necessary for this Intel AMT system. For more information, see: • About Maintenance Tasks on page 21 • Manual/Automatic Maintenance using the CLI on page 22
/AdminPassword <password>	The current password of the default Digest admin user defined in the Intel AMT device. This parameter is NOT necessary if any of these are true: • The RCS can find the Digest admin password (in one of the RCS profiles or using a Digest Master Password) • The user account running the RCS is a Kerberos account that is configured in the Intel AMT device with administrator permissions See Admin Password Parameter Errors on page 128 for information on errors resulting from this parameter.
/WMIUser <username>	The name (in the format domain\username) of a user with WMI permissions on the computer running the RCS. This parameter is only required when running the Configurator under a user without WMI permissions on the RCS computer.
/WMIUserPassword <password>	The password of the WMI user
/NetworkSettingsFile <file>	The path to a file that contains the network settings (FQDN and/or IP) to put in the Intel AMT device. Only use this parameter if you defined the source for at least one of these settings as a dedicated network settings file. For more information, see Defining IP and FQDN Settings on page 123.

/RCSBusyRetryCount <retries>	Defines the number of times to resend the request to the RCS if the RCS returns a status of busy. The maximum number of retries is 100. Each request is sent after a random period of time. If not supplied, the default for this parameter is 0.

6.13 Unconfiguring Intel AMT Systems

Command	Unconfigure
Description	Unconfigures Intel AMT. If the Intel AMT device is in admin control mode and an RCS address is provided, the Configurator sends the unconfiguration request to the RCS . Otherwise, unconfiguration is done locally, and for devices in client control mode the configuration status in RCS will be updated to "Unconfigured" if an RCS address is provided. There are two types of unconfiguration: • **Partial** – Removes the configuration settings from the system and disables the Intel AMT features on the system. The system and the RCS can still communicate since the PID, PPS, admin ACL settings, host name, domain name, and the RCS IP and port number are not deleted. Note that if the manufacturer defined the SOL and IDE interfaces to be closed by default, then a partial configuration operation will close them and they cannot be reopened without physical access to the Intel MEBX. This is a known Firmware limitation. • **Full** – Deletes all the Intel AMT settings from the system and disables the Intel AMT features on the system. **Note:** • Systems in Client Control mode are always unconfigured with a "Full" unconfiguration. • The default unconfiguration type for systems in Admin Control mode is "Partial".
Syntax	ACUConfig.exe [global options] UnConfigure [/AdminPassword <password>] [/RCSaddress <RCSaddress>] [/Full] [/ADOU <ADOU path>] {{[/DomainUser <username> [/DomainUserPassword <password>]} | [/DeleteADObjectViaRCS]} {[/WMIUser <username>] [/WMIUserPassword <password>]} [/SourceForAMTName <source>] [/NetworkSettingsFile <file>] [/RCSBusyRetryCount <retries>]
Parameters	

[global options]	See CLI Global Options on page 128
/AdminPassword <password>	The current password of the default Digest admin user defined in the Intel AMT device. This parameter is NOT necessary if any of these are true: • The Configurator/RCS can find the Digest admin password (in one of the RCS profiles or using a Digest Master Password) • The user account running the Configurator/RCS is a Kerberos account that is configured in the Intel AMT device with administrator permissions See Admin Password Parameter Errors on page 128 for information on errors resulting from this parameter.
/RCSaddress <RCSaddress>	The IP or FQDN of the computer running the RCS
/Full	For systems in Admin Control mode, does a full unconfiguration (the default is partial unconfiguration). Full unconfiguration also deletes customized data. For example: • Any root certificate hashes that were entered manually into the Intel MEBX • Any customized data that was pre-defined by the manufacturer (for example, the PKI DNS Suffix) **Note:** Do not use this parameter if your configuration flow relies on customized data. (For example, remote configuration of LAN-less systems into Admin Control mode requires a pre-defined customized value in the PKI DNS Suffix.)
/ADOU <ADOU path>	During unconfiguration, the Configurator deletes the Active Directory (AD) object that was created to represent the Intel AMT system. (The object was created by Intel SCS only if AD integration was enabled.) By default, the Configurator uses the settings configured in the Intel AMT device to find the location of the AD Organizational Unit (ADOU) containing the object. In large enterprise networks the search for the ADOU can take some time. If you supply this parameter, the Configurator will only look for the object in the Organizational Unit that you define in <ADOU path>.
/DomainUser <username>	The name (in the format domain\username) of a domain user with permissions to delete the AD object representing the Intel AMT system. If you supply this parameter, the AD object is deleted using the credentials of this user. **Note:** • For Intel AMT 6.2 and higher systems, by default, the credentials of the user running the Configurator are used to delete the AD object • For Intel AMT 6.1 and lower systems, the credentials of the user running the RCS are always used to delete the AD object

/DomainUserPassword <password>	The password of the domain user
/DeleteADObjectViaRCS	If you supply this parameter, the AD object is deleted using the credentials of the user running the RCS. **Note:** • For Intel AMT 6.2 and higher systems, by default, the credentials of the user running the Configurator are used to delete the AD object • For Intel AMT 6.1 and lower systems, the credentials of the user running the RCS are always used to delete the AD object
/WMIUser <username>	The name (in the format domain\username) of a user with WMI permissions on the computer running the RCS. This parameter is only required when running the Configurator with a user without WMI permissions on the RCS computer.
/WMIUserPassword <password>	The password of the WMI user
/SourceForAMTName <source>	Defines how the FQDN (hostname.suffix) for the Intel AMT device is constructed. Valid values: • DNS — The hostname part of the FQDN is the hostname from the host operating system. The suffix is the "Primary DNS Suffix" from the host operating system. This is the default setting, and is correct for most network environments. • SpecificDNS — The hostname part of the FQDN is the hostname from the host operating system. The suffix is the "Connection-specific DNS Suffix" of the on-board wired LAN interface. • AD — The hostname part of the FQDN is the hostname from the host operating system. The suffix is the AD domain of which the host operating system is a member. • DNSLOOKUP — Takes the FQDN returned by an "nslookup" on the IP address of the on-board wired LAN interface. To use this option, the DNS must be configured correctly with Reverse Lookup Zones. • HOST — Takes the hostname from the host operating system. The suffix is blank. **Note:** When this parameter is not supplied, the default source for the FQDN is "DNS". However, if the /NetworkSettingsFile parameter is supplied (and FQDN data is included in the file), the FQDN is taken from the file.
/NetworkSettingsFile <file>	This parameter tells the Configurator to get the IP and/or the FQDN from a dedicated network settings file. For information about the required XML format, see the NetworkSettings.xml example file located in the sample_files folder.

/RCSBusyRetryCount <retries>	Defines the number of times to resend the request to the RCS if the RCS returns a status of busy. The maximum number of retries is 100. Each request is sent after a random period of time. If not supplied, the default for this parameter is 0.

6.14 Moving from Client Control to Admin Control

Command	MoveToACM
Description	This command modifies the Intel AMT device by changing it from Client Control mode to Admin Control mode. When complete, the security related limitations of the Client Control mode no longer apply to this system (see Control Modes on page 15). To use this command: • The system must be configured in Client Control mode. • The Intel AMT system and the RCS must be setup for authentication using remote configuration certificates. For more information, see Setting up Remote Configuration on page 208. **Note:** • This command is only supported on Intel AMT 7.x and higher. • For Intel AMT 10.0 or later LAN-less systems, you can use this command as part of the remote configuration process (see Configuration of LAN-less Platforms on page 7). As an alternative for this command, you can do this: 1. Unconfigure the system. 2. Configure the system again using a method that uses the RCS to put the system in the Admin Control mode during configuration. **Note:** This alternative is not relevant for LAN-less systems.
Syntax	ACUConfig.exe [global options] MoveToACM <RCSaddress> {[/WMIUser <username>] [/WMIUserPassword <password>]} [/AdminPassword <password>] [/CertificateCNSuffix <suffix>] [/SourceForAMTName <source>] [/RCSBusyRetryCount <retries>]
Parameters	
[global options]	See CLI Global Options on page 128
<RCSaddress>	The IP or FQDN of the computer running the RCS

/WMIUser <username>	The name (in the format domain\username) of a user with WMI permissions on the computer running the RCS. This parameter is only required when running the Configurator with a user without WMI permissions on the RCS computer.
/WMIUserPassword <password>	The password of the WMI user
/AdminPassword <password>	The current password of the default Digest admin user defined in the Intel AMT device. This parameter is NOT necessary if any of these are true: • The Configurator/RCS can find the Digest admin password (in one of the RCS profiles or using a Master Password) • The user account running the Configurator/RCS is a Kerberos account that is configured in the Intel AMT device with administrator permissions See Admin Password Parameter Errors on page 128 for information on errors resulting from this parameter.
/CertificateCNSuffix <suffix>	When the MoveToACM command starts, the Configurator sends all the hashed root certificates located in the Intel AMT device to the RCS. The RCS looks in the certificate store of the user account running the RCS for a remote configuration certificate that traces to one of the hashes. For authentication to succeed, the domain suffix of the Common Name (CN) in the Subject Name field of the certificate must match one of these: • For systems with an on-board wired interface — It must match the "Connection-specific DNS Suffix" assigned to the Intel AMT device. This suffix can be assigned to the device using option 15 of the DHCP server (DNS Domain Name). • For Intel AMT 10.0 or later LAN-less systems — It must match the PKI DNS Suffix pre-defined in the Intel MEBX by the manufacturer/supplier of the Intel AMT system. By default, the RCS tries to authenticate using only the first certificate it finds that matches one of the hashes. If this is not the correct certificate (for example, in networks using multiple remote configuration certificates with different domain suffixes), authentication will fail. You can use this parameter to specify the correct DNS Domain Name that is assigned to the Intel AMT device. If supplied, the RCS examines each remote configuration certificate in the store until it finds a certificate with this suffix in the CN.

/SourceForAMTName <source>	Defines how the FQDN (hostname.suffix) for the Intel AMT device is constructed. Valid values: • DNS — The hostname part of the FQDN is the hostname from the host operating system. The suffix is the "Primary DNS Suffix" from the host operating system. This is the default setting, and is correct for most network environments. • SpecificDNS — The hostname part of the FQDN is the hostname from the host operating system. The suffix is the "Connection-specific DNS Suffix" of the on-board wired LAN interface. • AD — The hostname part of the FQDN is the hostname from the host operating system. The suffix is the AD domain of which the host operating system is a member. • DNSLOOKUP — Takes the FQDN returned by an "nslookup" on the IP address of the on-board wired LAN interface. To use this option, the DNS must be configured correctly with Reverse Lookup Zones. • HOST — Takes the hostname from the host operating system. The suffix is blank.
/RCSBusyRetryCount <retries>	Defines the number of times to resend the request to the RCS if the RCS returns a status of busy. The maximum number of retries is 100. Each request is sent after a random period of time. If not supplied, the default for this parameter is 0.

6.15 Disabling Client Control Mode

Command	DisableClientControlMode

Description	Permanently disables the Client Control mode option in the Intel AMT device (see Control Modes on page 15). After running this command, the device cannot be changed back to the Client Control mode. After you run this command: • Client Control mode can only be re-enabled from the BIOS of the computer. (Either by resetting the BIOS, or using a manufacturer provided BIOS menu command to re-enable the option.) • Future configuration methods on an unconfigured device can only put the device in Admin Control mode. • You cannot use this command on a system that is configured in Admin Control mode. • If a device is configured in Client Control mode and the `disableclientcontrolmode` command is used, the confirmation status of the device will not change, reconfiguring the device will not change the control mode, and the system will need to be unconfigured before Client Control mode is disabled. • It is recommended to run `disableclientcontrolmode` on an unconfigured device. • WARNING: Not all platforms can re-enable CCM once disabled.
Syntax	ACUConfig.exe [global options] DisableClientControlMode `ACUConfig.exe [global options] DisableClientControlMode [/confirmDisableCCM]`
Parameters	
`[global options]`	See CLI Global Options on page 128 /confirmDisableCCM : Skip the confirmation-request that appears in the command, agreeing that you understand the warning attached to this command.
`/confirmDisableCCM`	Skip the confirmation-request that appears in the command, agreeing that you understand the warning attached to this command.

6.16 Sending a Hello Message

Command	`SendHello`

Description	Sends a "Hello" message to the RCS. This option is relevant only if you want to use scripts to configure the system (see Remote Configuration Using Scripts on page 216). To enable configuration using scripts, go to the Advanced Configuration Options on page 78 and select the **Support Configuration triggered by Hello messages** option. A sample script, based on configAMT.bat, is provided in the Intel® SCS download package under \sample_files\hello_listener_sample_files\.
Syntax	`ACUConfig.exe [global options] SendHello <RCSaddress> [<port>]`
Parameters	
`[global options]`	See CLI Global Options on page 128
`<RCSaddress>`	The IP or FQDN of the computer running the RCS
`<port>`	The port number used by the RCS to listen for Hello messages. If not supplied, the message is sent to the default port (9971).

6.17 Disabling the EHBC Option

Command	`DisableEmbeddedHBC`
Description	Permanently disables the Embedded Host Based Configuration (EHBC) option in the Intel AMT device. After running this command, the EHBC option cannot be used on the device. After you run this command: • The EHBC option can only be re-enabled on the device by the computer manufacturer or supplier • The control mode and configuration status of a device that is already configured is not changed • If the device is already configured, you cannot reconfigure the device directly to Client Control mode. You must first unconfigure the device and then reconfigure it with the control mode that you want. **Note:** The EHBC option is only available on Intel AMT systems that were prepared by the manufacturer/supplier to include the EHBC option. The EHBC option was created to make it easier to configure and manage Intel AMT devices that are embedded in unattended systems. For example, a device that is embedded in an Automated Teller Machine (ATM). For more information about the EHBC option, contact your computer manufacturer or supplier.

Syntax	`ACUConfig.exe [global options] DisableEmbeddedHBC`
Parameters	
`[global options]`	See CLI Global Options on page 128

6.18 Running Scripts with the Configurator/RCS

Intel SCS include options that you can use to run scripts. These scripts can be batch files or executables created using scripting languages. Before the script starts to run, the Configurator/RCS sends parameter values about the Intel AMT system to the script. The script can then use these parameter values. For example, you could use a script to send data to your management console about each Intel AMT system after it is configured.

Note:

The parameter values are sent as a string. Parameters without values are sent as empty strings. Each parameter value is separated by a space.

The Configurator and the RCS support scripts differently (the RCS also sends additional parameters to the scripts).

For more information, see:

- Scripts Run by the RCS below
- Scripts Run by the Configurator on page 150
- Who Runs the Scripts? on page 151
- What if a Failure Occurs? on page 152
- Script Runtime and Timeout on page 153
- Parameters Sent in Base64 Format on page 153
- Script Authentication Mechanism on page 153

6.18.1 Scripts Run by the RCS

The RCS supports three different scripts:

- Script #1: Runs after configuration, reconfiguration, and maintenance operations
- Script #2: Runs before unconfiguration operations
- Script #3: Runs after unconfiguration operations

You can define which of these scripts the RCS will use and where they are located. The scripts can be located on any computer in the network that the RCS can access. The scripts are defined via the Console in the Configuration Scripts tab (see Defining the RCS Settings on page 77).

Note:

- Make sure that the RCS has read and execute permissions on the scripts and the folder where the scripts are located.
- Scripts #2 and #3 will NOT run on systems with Intel AMT 6.2 and higher if they are configured in Client Control mode. This is because for these systems unconfiguration is always done locally by the Configurator. Also, the `Unconfigure` command does not support the `/FileToRun` parameter used by the Configurator to run scripts locally.

This table describes the parameters and the sequence in which the RCS sends them to script #1.

Table 6-1: Parameters Sent by the RCS to Script #1

#	Description
1	The type of operation that was done on the Intel AMT device: • 1 = Configuration • 2 = Reconfiguration • 3 = Maintenance
2	The status of the operation: • 0 = Succeeded • 32 = Completed with warnings
3	The FQDN defined in the Intel AMT device
4	The IP address defined in the Intel AMT device
5	The UUID of the Intel AMT device
6	The Intel MEBX password of the Intel AMT device*
7	The password of the default Administrator ("admin") user in the Intel AMT device*
8	The RFB password defined in the Intel AMT device for port 5900*
9	The name of the configuration profile used by the RCS
String Example: `1 0 "myamtname.example.com" "192.168.1.10" "88888888-8887-8888-8888-878888888888" "mebxpassword" "adminpassword" "rfbpassword" "Profile1"` (Parameters marked with an asterisk (*) are sent to the script in Base64 format)	

This table describes the parameters and the sequence in which the RCS sends them to scripts #2 and #3.

Table 6-2: Parameters Sent by the RCS to the Scripts #2 and #3

#	Description
1	The FQDN defined in the Intel AMT device
2	The UUID of the Intel AMT device

6.18.2 Scripts Run by the Configurator

Scripts run by the Configurator are only run on Intel AMT systems that support host-based configuration (Intel AMT 6.2 and higher). The script must be put in a location that the Configurator can access from the Intel AMT system. The Configurator can run a script after configuration, reconfiguration, and maintenance operations done with these commands:

- `ConfigAMT`
- `MaintainAMT`

This table describes the CLI parameters of these commands used to run scripts.

Table 6-3: CLI Parameters

Parameter	Description
`/FileToRun <filename>`	If this parameter is supplied, the Configurator will run this executable file (batch, script, or executable) after the command has completed. If the `/FileToRun` parameter is used without the `/LowSecurity` global option, the file must be digitally signed (see Digital Signing of Files on page 12). If the file is not signed, the Configurator will NOT run the CLI command or the file. In addition, if the `/LowSecurity` parameter is not used, the file must be located in the same folder as the `ACUConfig.exe` file. The default installation path of `ACUConfig.exe` is "`C:\Program Files (x86)\Intel\SCS ACUConfig`".
These additional optional parameters are valid only if `/FileToRun` was specified:	
`/FileHash <SHA256 hash>`	When this parameter is supplied, the Configurator runs a hash function on the file supplied in the `/FileToRun` parameter. The result of the hash function is then compared with the original hash value of the file, supplied in this parameter. If the values of the hashes are different, the Configurator will NOT run the CLI command or the file. (If any change was made to the file, the hash values will not be the same.) Before you can use this option, you must generate a SHA256 hash value from the `<filename>` file. The `sample_files` folder includes an application (`SHA256.exe`) that you can use to generate the hash value. For example: `SHA256.exe MyFile.bat` will return the hash value of `MyFile.bat`. The hash value is marked in blue. Copy the value and supply it in the `<SHA256 hash>` parameter.

Parameter	Description
/FileUser <password>	It is recommended to use this parameter to supply a user with the minimum permissions required to run this file.
/FilePassword <password>	Contains the password required to run the file. Valid only if /FileUser was also specified.

This table describes the parameters and the sequence in which the Configurator sends them to the file that you specify in the /FileToRun parameter.

Table 6-4: Parameters Sent by the Configurator to the Script

#	Description
1	The user defined in the /FileUser parameter*
2	The password defined in the /FilePassword parameter*
3	The hostname defined in the Intel AMT device
4	The FQDN defined in the Intel AMT device
5	The UUID of the Intel AMT device
6	The Intel MEBX password of the Intel AMT device*
7	The password of the default Administrator ("admin") user in the Intel AMT device*
String Example: fileusername fileuserpassword myhostname myhostname.example.com 88888888-8887-8888-8888-878888888888 mebxpassword adminpassword (Parameters marked with an asterisk (*) are sent to the script in Base64 format.)	

6.18.3 Who Runs the Scripts?

Scripts are usually run by the component (Configurator/RCS) that does the requested operation. But, the Intel AMT version, the command you use, and the control mode can all cause different scripts to run.

Intel AMT 6.1 and Lower

Operations on these systems can only be done remotely by the RCS. This means that scripts are always run only by the RCS. The Configurator scripts and the /FileToRun parameter (if supplied) are always ignored.

Intel AMT 6.2 and Higher

Operations on these systems can be done by the Configurator or the RCS.

- If you use the `ConfigViaRCSOnly` or `MaintainViaRCSOnly` commands, only the RCS scripts are run.
- If you use the `MaintainAMT` command the Configurator scripts will run only if the `/FileToRun` parameter is used. (The RCS scripts are not supported.)
- If you use the `ConfigAMT` command:
  - The Configurator scripts will run only if the `/FileToRun` parameter is used.
  - On unconfigured systems, if the control mode setting in the XML profile is defined as Admin Control mode the RCS scripts will run.

  This means that if the `/FileToRun` parameter is used and the control mode is Admin Control mode, two scripts will run for the system.

6.18.4 What if a Failure Occurs?

If a script defined to run before an unconfiguration operation fails, the unconfiguration operation is canceled. Scripts defined to run after configuration, reconfiguration, maintenance, and unconfiguration operations only run if the operation is successful (or completes with warnings). By default, if the script fails, Intel SCS does not make any changes to the Intel AMT settings set by the operation that ran before the script. "Script failure" means that your script returned a non zero exit code, or Intel SCS did not succeed to run the script.

But leaving Intel AMT configured after a post configuration script fails might not be the result you want. If it is critical that your post configuration script will complete successfully, you might prefer to have Intel AMT unconfigured if the script fails.

For post configuration scripts run by the RCS, you can define this by selecting the **Unconfigure Intel AMT if the script fails** check box. When this check box is selected, the RCS will automatically unconfigure Intel AMT if the script fails after any configuration, reconfiguration, or maintenance operation. Note that unconfiguration is not activated for errors returned because the script did not complete within the maximum permitted runtime.

For post configuration scripts run by the Configurator, you can define this using the `/AbortOnFailure` parameter. When this parameter is supplied, the Configurator will automatically unconfigure Intel AMT if the configuration operation fails or the post configuration script fails. But unconfiguration will only occur if the Intel AMT system was in an unconfigured state when the configuration operation started. The `/AbortOnFailure` parameter is ignored for reconfiguration and maintenance operations.

6.18.5 Script Runtime and Timeout

The maximum permitted runtime for scripts is 60 seconds. If the script does not complete within 60 seconds, the operation that was running when the script was called will return a warning. The warning is recorded in the log file and will contain an error code (0xC0003EAA) and a description like this:

> "The supplied script has not finished in the time-out period defined by Intel® SCS"

But for scripts that run before unconfiguration operations, if the script does not complete within 60 seconds an error is returned. This error will prevent the unconfiguration operation from starting.

For scripts run by the RCS you can change the maximum permitted runtime. To do this, enter the new value in the **Maximum time for script execution (in seconds)** field on the Configuration Scripts tab. The minimum value is 1 second and the maximum value is 3600 seconds.

Changing the maximum permitted runtime is not possible for scripts run by the Configurator. If your script requires more than 60 seconds to complete, you can wrap your script with a batch file like this:

```
Start Myscript.bat %1 %2 ...
Exit 0
```

This will cause the operation to return a success code (0). If you do this, your script will be responsible to handle any subsequent errors if they are generated by your script. Script errors will not be recorded in the log.

6.18.6 Parameters Sent in Base64 Format

Some of the parameters sent by the Configurator/RCS are sent in Base64 format.

The number of characters sent in the Base64 value representing the parameter must be divisible by 4. If it is not, additional "=" characters are added to the end of the Base64 value. For example, if the Base64 value includes only 6 characters two "=" characters are automatically added.

When Base64 values are sent to a batch file, the command line interpreter removes these additional "=" characters. This means that the parameter value cannot be decoded correctly. To solve this problem, add the missing "=" characters to the Base64 value before decoding it.

6.18.7 Script Authentication Mechanism

By default, the RCS does not authenticate the scripts defined via the Console in the Configuration Scripts tab. The RCS will run the scripts that you define, regardless of the content or status of the script file. This default behavior assumes that your network environment setup will prevent attackers from accessing the computer(s) where the RCS and the scripts are located.

If you want to increase security when running scripts, you can enable a script authentication mechanism. To enable this mechanism, select the **Enable script authentication mechanism** check box in the Configuration Scripts tab.

If you want to use this mechanism:

- All scripts that you define in the Configuration Scripts tab must be digitally signed using a Microsoft Authenticode certificate. To make sure that your scripts are signed correctly, use the PowerShell command named `Get-AuthenticodeSignature`. The script authentication mechanism of RCS only supports scripts that can be successfully validated using this command.
- You must make sure that only authorized code signing certificates are trusted by the operating system where the RCS is running
- Script files that cannot be signed, for example batch files, are not permitted
- VBScript files (*.vbs) are not supported when using this mechanism

When this mechanism is enabled:

- Each time the RCS starts, the RCS will try to authenticate all the scripts defined in the Configuration Scripts tab. Also, immediately before running any of these scripts, the RCS will try to authenticate the script. The RCS will only run the script if the digital signature is authenticated successfully.
- Before starting any RCS operation for which a script has been defined to run (before or after the operation), the RCS first tries to authenticate the script. If authentication fails, the associated RCS operation is canceled and does not run.
- When the **Unconfigure Intel AMT if the script fails** check box is selected, the RCS will try to authenticate all the scripts defined in the Configuration Scripts tab. If authentication of any of the scripts fails, the RCS operation (configuration, reconfiguration, or maintenance) is canceled and does not run. This also means that the script is canceled and no changes are made to the current Intel AMT settings (Intel AMT will not be unconfigured.)
- In addition, when a script fails authentication, the RCS operation for which the script is defined is suspended. All future requests for that type of operation that are sent to the RCS will be denied. Normal functionality for this operation will only be restored after the cause of the authentication failure is fixed.
- For each script authentication failure, the RCS will return an error message and record an error in the log

Note:

The scripts authentication mechanism is only available for scripts run by the RCS. If you are using scripts run by the Configurator, you can use the `/FileHash` parameter instead (see Scripts Run by the Configurator on page 150).

6.19 Configurator Return Codes

This table describes the return codes that are shown and recorded in the log file when running Configurator CLI commands.

Table 6-5: Configurator Return Codes

#	Description
0	The requested operation completed successfully
1	Intel AMT is already configured on this system

#	Description
2	Intel AMT is already unconfigured on this system
3	This system does not have Intel AMT (or it is disabled in the Intel MEBX, or the correct drivers are not installed or enabled)
4	This system supports Intel® Small Business Advantage (Intel® SBA) and cannot be configured by Intel SCS components. Intel SBA systems were specifically designed for small businesses, and can only be configured using the software included with Intel SBA.
6	The RCS failed to process the request
7	The Intel AMT device does not have a PSK (prerequisite for the requested operation)
8	Invalid command parameter
9	The system is not in Intel AMT mode (check the manageability setting in the Intel MEBX)
10	The manageability mode has been changed to "AMT". You must reboot the system to complete this operation.
11	Failed to change to Intel AMT mode (check the manageability setting in the Intel MEBX)
12	An internal error has occurred in Intel AMT
16	Invalid format used in the new Intel MEBX password parameter (refer to the documentation)
17	Invalid format used in the current Intel MEBX password parameter (refer to the documentation)
22	An internal exception occurred when processing the request
25	The system is already in Intel AMT mode
26	The `UsingDHCP` parameter was supplied, but DHCP is not active on the host operating system
27	Access denied. Make sure that the user has administrator permissions on the local host or in the Intel AMT device.
30	This Intel AMT device does not support host-based configuration
31	This Intel AMT device is in a state that does not support the `ConfigAMT` command
32	The requested operation completed, but with warnings
33	Failed to configure this Intel AMT device
34	Failed to do the requested operation. The flash wear-out protection mechanism limits consecutive operations in a certain time period. Try the operation again later.
35	A certificate request was sent to the Certification Authority but the created certificate was put into "Pending Requests" waiting for approval. Intel SCS does not support pending requests.
36	Failed to request the certificate

#	Description
37	Failed to parse the XML file (possible reasons- the file does not exist or access to it is denied; the file contains incorrect parameters; incorrect or missing encryption password/parameter); XML file is encrypted using discontinued algorithm (see Error with XML File or Missing SCSVersion Tag on page 222)
38	Error with XML file (possible reasons- the file does not exist or access to it is denied; the file contains incorrect parameters; incorrect or missing encryption password/parameter; invalid data)
39	The Intel AMT device is in a state that does not support disabling the Client Control mode
40	This system was already unconfigured. The system was successfully put in the "Pre Provisioned" state and the Intel AMT interfaces are now closed.
41	The certificate cannot be retrieved because access to the Certification Authority is denied
42	Failed to write to the file. A possible reason is insufficient permissions in the selected folder.
43	Failed to read from the given file. A possible reason is insufficient permissions in the selected folder.
44	Memory Allocation Error
45	Failed to unconfigure this Intel AMT device or Intel AMT unconfiguration failed
46	Settings defined in the dedicated network settings XML file are not compatible with the network settings defined in the configuration profile
49	Failed to do the requested maintenance tasks on this Intel AMT device
50	The Intel AMT device is in a state that does not support the `Maintenance` command
51	TLS cannot be configured because cryptography is disabled on this system
54	The Intel AMT device cannot be set with the host FQDN and a dedicated FQDN
55	The Intel AMT device cannot be set with the host IP and a dedicated IP
56	An FQDN is mandatory for configuration (supply the FQDN in the NetworkSettings tag of the profile)
57	Setting a static IP to the Intel AMT device from the host dynamic IP is not permitted
58	When defining a static address, the IP and subnet mask parameters are mandatory
59	Failed to find the host IP address and subnet mask to set in the Intel AMT device (possible reasons - the network card is disabled; the network connection is disabled; the network cable is unplugged)
60	Dedicated FQDN is not permitted
61	An invalid IP address was supplied in the parameter
62	Cannot configure an AD object or certificates for the Intel AMT device without a valid FQDN
65	Administrator credentials must be supplied in the XML or CLI to configure the Intel AMT device

#	Description
66	Failed to reissue certificates because the certificate data is missing in the profile
67	Failed to renew the AD password because the AD data is missing in the profile
68	Invalid parameter was found
70	Failed to connect to the Intel AMT device (possible reasons: the system does not have Intel(R) AMT or is not responding; user access to it is denied)
71	The buffer maximum size supplied in the function is too small
73	Failed to put the system in the "Pre Provisioned" state (you can try to unconfigure the system using the Intel MEBX "Full Unprovision" option)
74	Failed to complete the Setup operation on this Intel AMT device
75	Failed to complete remote configuration of this Intel AMT device
76	The file supplied in the `FileToRun` parameter returned an error when it was run
77	Missing mandatory parameter
78	Failed to put the Intel AMT device in the "In Provision" state. The Start Configuration operation failed. Examine the Intel MEBX settings to make sure remote configuration is enabled, or a TLS PSK pair is defined.
79	Failed to connect to the Intel Management Engine Interface PTHI client
80	Failed to complete the System Discovery
81	Failed to run the file supplied in the `FileToRun` parameter
82	The `FileToRun` parameter is not permitted for configuration methods using a Remote Configuration Server
83	The Intel Management Engine Interface driver is not installed or cannot be accessed
84	Invalid data in the profile
85	Failed to move the Intel AMT device to Admin Control mode
86	Failed to get the FQDN
87	Failed to verify the signature of the file supplied in the `FileToRun` parameter. To cancel this verification, run the command using the `LowSecurity` global option.
88	The requested operation was aborted because required file access failed
89	The file supplied in the `FileToRun` parameter is not located in a trusted location. To cancel this prerequisite, run the command using the `LowSecurity` global option.

#	Description
90	Failed to get the Digest admin password to put in the Intel AMT device (calculated by the RCS using the Digest Master Password)
91	Failed to get the Digest admin password that is configured in the Intel AMT device
92	Failed to send the Hello Message to the RCS
93	Failed to submit the certificate request to the Certification Authority
94	Failed to get the certificate
95	Failed to generate a TLS-PSK Pair
96	Failed to generate the PKCS10 request
97	Failed to get the FQDN of the Intel AMT device
98	Failed to get the IP address of the Intel AMT device
99	Failed to get the UUID of the Intel AMT device
100	Failed to get the FQDN and the IP address of the Intel AMT device
101	The remote configuration operation completed, but with warnings
102	Failed to retrieve the PID from this Intel AMT device
103	The requested functionality is not supported on this operating system
104	Failed to renew the Digest admin password in the Intel AMT device because the administrator password is missing in the profile
105	Failed to read data from the registry. A possible reason is that the registry value does not exist or access to it is denied.
106	Failed to verify the hash of the file supplied in the `FileToRun` parameter against the Hash supplied in the `FileHash` parameter
107	The `Notify RCS` operation failed
108	This Intel AMT system already exists in the database
109	Failed to connect to the RCS
110	Failed to verify the file signature chain. Either connect the computer to the Internet, or manually download and install the root certificate update package from the Microsoft update catalog.
111	The detected version of the Management Engine (ME) firmware is considered vulnerable for Intel-SA-00075. It is highly recommended that you upgrade your ME firmware. Read the Public Security Advisory at https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00075.html for more information.

Chapter 7

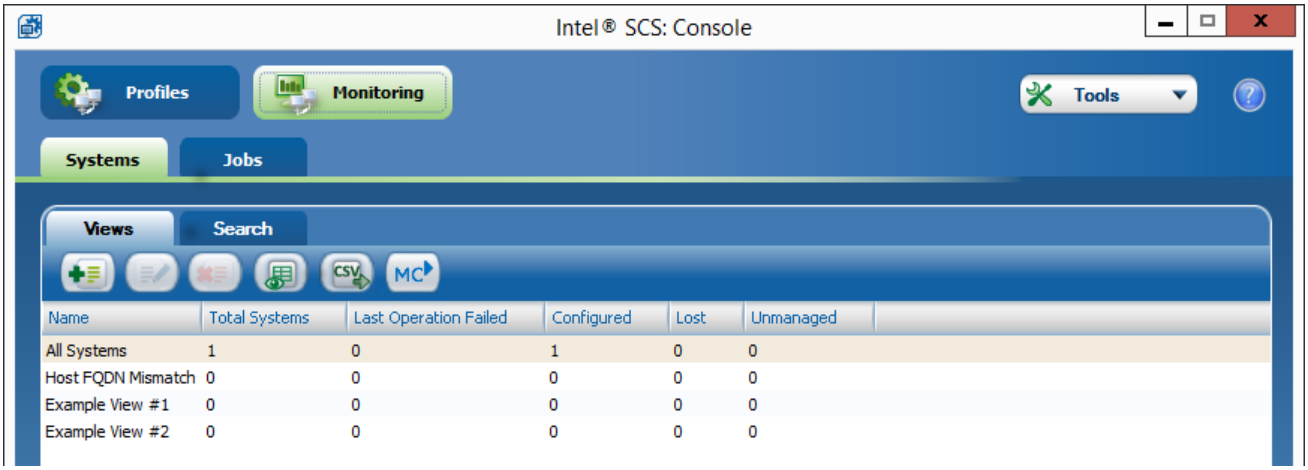
Monitoring Systems

This chapter describes how to use the monitoring options, available from the Console, when working in database mode.

For more information, see:

7.1 About Monitoring Intel AMT Systems

In database mode, during configuration data about each Intel AMT system is stored in the database. You can use the Monitoring options in the Console to send WMI Query Language (WQL) queries to the database about these systems.



Example of Views

This table describes the options available from the **Monitoring** > **Systems** tab.

Use this...	To do this...
Views Tab	To define and save multiple queries, also known as "Views". You can use these views to filter Intel AMT systems into logical groups. For more information, see: • Creating a View on page 162 • Viewing Systems on page 165 • Viewing Systems Using the Intel® Manageability Commander Tool on page 169 The Views tab also includes these built-in default views: • **All Systems** – All systems that exist in the database. • **Host FQDN Mismatch** – See Detecting and Fixing Host FQDN Mismatches on page 172. (You cannot edit or delete these default views.)
Search Tab	To quickly find a specific system or group of systems. For more information, see: Searching for a System on page 166.

Note:

You can also use the Views tab and the Search tab, to get data about operation logs and the admin password. For more information, see:

- Getting the Admin Password on page 174
- Viewing Operation Logs on page 175

7.2 About Adding and Deleting Systems

You can only use the Console to monitor and maintain systems that exist in the database.

These CLI configuration commands automatically add the systems to the database:

- `ConfigViaRCSOnly` – When you configure systems using this command, they are always added to the database. For information about how to use this command, see Configuring Systems using the RCS on page 134.
- `ConfigAMT` – This command uses an XML profile as part of the unified configuration process. In some conditions, this command does not add the system to the database:
  - **Intel AMT 6.1 and lower** – These systems are always added to the database.
  - **Intel AMT 6.2 and higher** – These systems are added to the database only if the XML profile is defined to put the Intel AMT device in Admin Control mode. This is defined when the profile is exported from the Console. When you export the profile, select the **Put locally configured devices in Admin Control mode**. check box (see Exporting Profiles from the Console on page 83.)

    For information about how to use this command, see Configuring Systems (Unified Configuration) on page 132.

Intel SCS includes an additional CLI command (`NotifyRCS`) that you can use to manually add configured systems to the database. If you have systems that are already configured, but not in the database, you can use this command to add them to the database. You can also use this command to add systems that were configured in Client Control mode using `ConfigAMT`. For information about how to use this command, see section Adding a Configured System or Updating an Unconfigured System on page 135.

If necessary, you can delete systems from the database. For example, when computers are moved, or changes are made to the network, the RCS might lose connection with some systems. The Console can only run jobs and operations on systems to which the RCS can connect.

To delete a system:

1. In the Console, click **Monitoring** and select the **Systems** tab.
2. Locate and select the systems using the Views tab or the Search tab.
3. Right-click and select **Delete System**.

> **Note:**
>
> You cannot delete a system if it is part of a job, and the job is in one of these statuses: "Aborting", "In Progress", and "Loading".

7.3 Creating a View

A "view" is a query defined using the WMI Query Language (WQL). You can create several views using different conditions to filter the Intel AMT systems into logical groups.

To create a view:

1. In the Console, click **Monitoring**.
2. Select the **Systems** > **Views** tab and click  . The View Definition window opens.

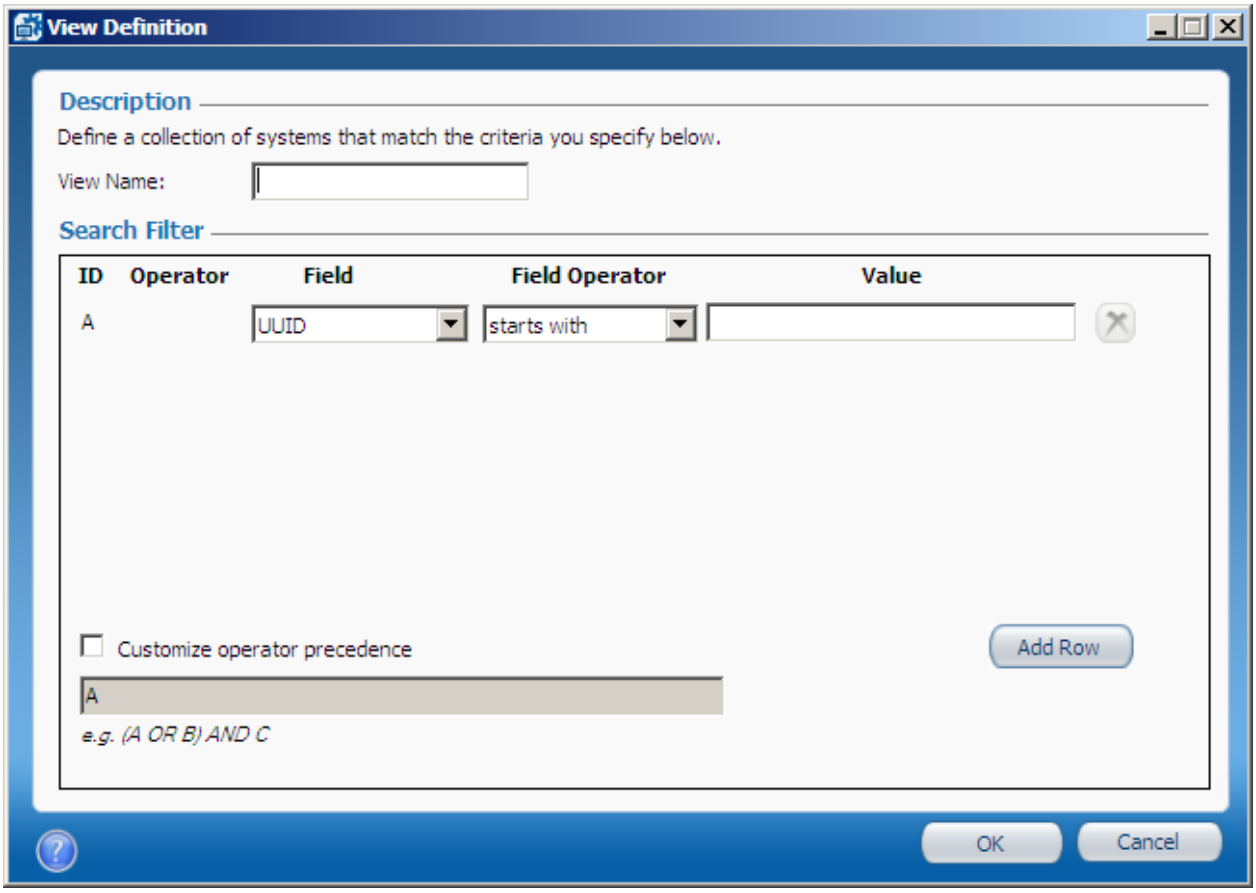


Figure 7-1: View Definition Window

3. In the View Name field, enter a descriptive name for this view.
4. Define the filter conditions as described in Defining a System Filter on the next page.
5. Click **OK**. The View Definition window closes and the view is added to the list of views.

7.3.1 Defining a System Filter

The search filter defines which systems are included in a view. A job can be defined based on an existing view or a search filter that you define in the job. When you create a view or a job, the systems that match the filter are added to the view/job.

To define a system filter:

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

Table 7-1: System Filter Options

Field	Field Operator	Value
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
Intel AMT FQDN		A string containing the required part of the FQDN defined in the Intel AMT device that you want to include in the filter
Intel AMT IPv4		A string containing the required part of the IPv4 address of the wired LAN interface defined in the Intel AMT device that you want to include in the filter
Version		The Intel AMT version
Last Configuration Time	• >= • <	By default, the Value field of these options contains the current date and time. 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		
Last Action	in	From the drop-down list, select one or more of the states (see Last Action and Configuration Status on page 180). 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)
Managed State	in	The managed state: • Managed • Unmanaged For more information, see Changing the Managed State of Systems on page 171. **Note:** This field is not available in Jobs.
Host FQDN State	in	See Detecting and Fixing Host FQDN Mismatches on page 172

2. Optionally, define more filter conditions:

   a. Click **Add Row**. A new filter condition row is added under the existing row.

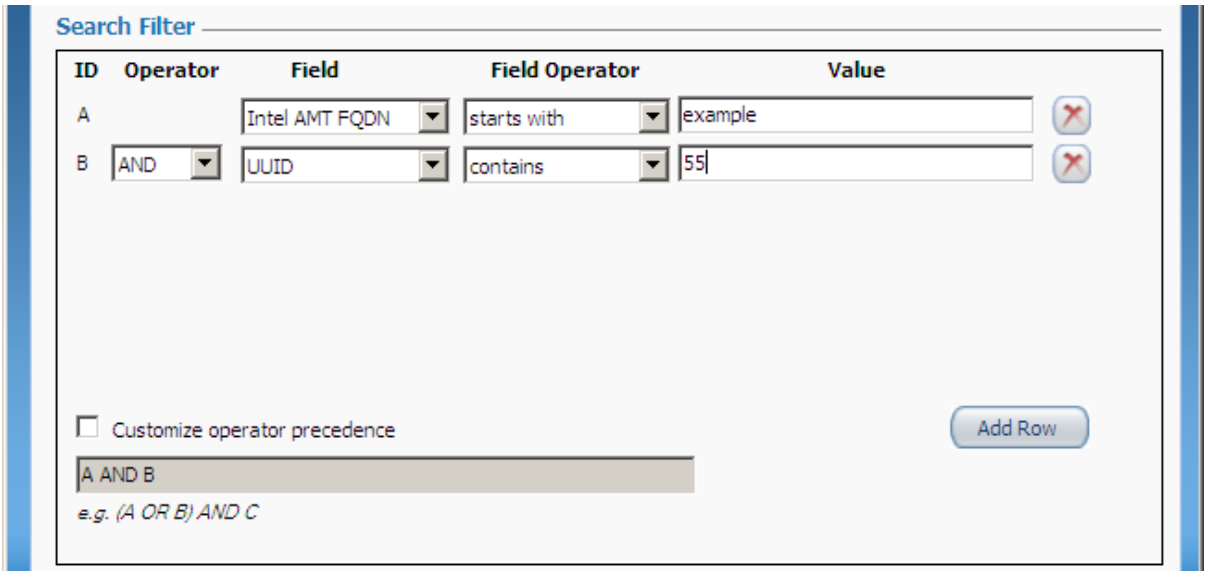


   Figure 7-2: System Filter Example

   b. From the first drop-down list, select one of these 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 step 1.

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

> **Note:**
>
> You can delete a condition by clicking the icon next to the condition.

3. (Optional) You can also customize the operator precedence of the filter condition rows. To do this:

   a. Select the **Customize Operator Preference** check box.

   b. Add brackets to the condition ID codes (A, B etc.) to make the changes that you want to the filter.

7.4 Viewing Systems

The **Systems** > **Views** tab shows a summary of the number of systems that each view contains. The systems are automatically sorted into these columns in the view:

- **Total Systems** – The total number of systems in the view
- **Last Operation Failed** – The number of systems for which the RCS did not successfully complete the last operation
- **Configured** – The number of systems for which configuration completed
- **Lost** – The number of systems to which the RCS could not successfully connect during the last operation
- **Unmanaged** – The number of systems in the "Unmanaged" state

For each view (and column in a view) you can get data about the systems it contains.

To get data about systems:

1. In the Console, click **Monitoring** and select the **Systems** > **Views** tab.
2. Select the view for which you want to get details about the systems that it contains.
3. Select a column in the view, right-click, and select one of these:
   - **Show Systems** – Shows all the systems in the view. For the Total Systems and Name columns, this is the only available option.
   - **Show Systems (this column only)** – Shows only the systems that are in the column that was selected

   The List of Systems window opens.

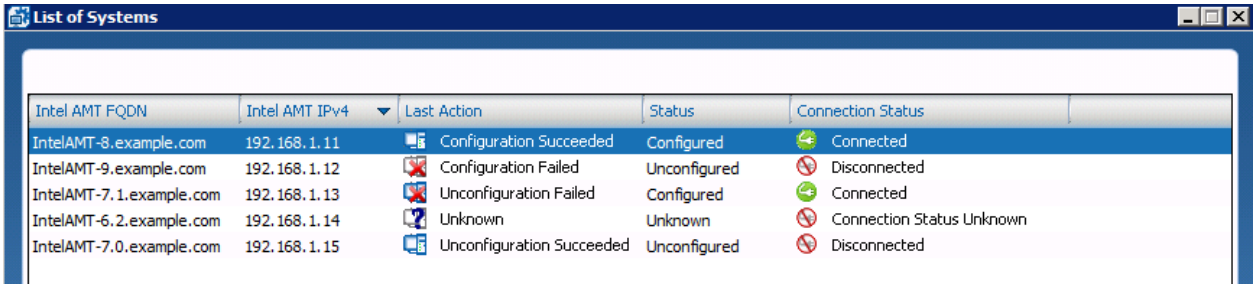


Figure 7-3: List of Systems Window

4. Click a system in the list. Data for the selected system is shown in the bottom section of the List of Systems. The profile that was used during the last configuration/reconfiguration operation is shown as a link. You can view the profile details by clicking the link.

   For information about other options available from the List of Systems, see:

   - Sorting the List of Systems on page 168
   - Getting the Admin Password on page 174
   - Viewing Operation Logs on page 175

   For a list of the possible statuses, see Last Action and Configuration Status on page 180.

7.5 Searching for a System

The Search tab lets you quickly send a query to the database to find a specific Intel AMT system or systems.

To search for systems:

1. In the Console, click **Monitoring** and select the **Systems** > **Search** tab.

   The Search tab opens.

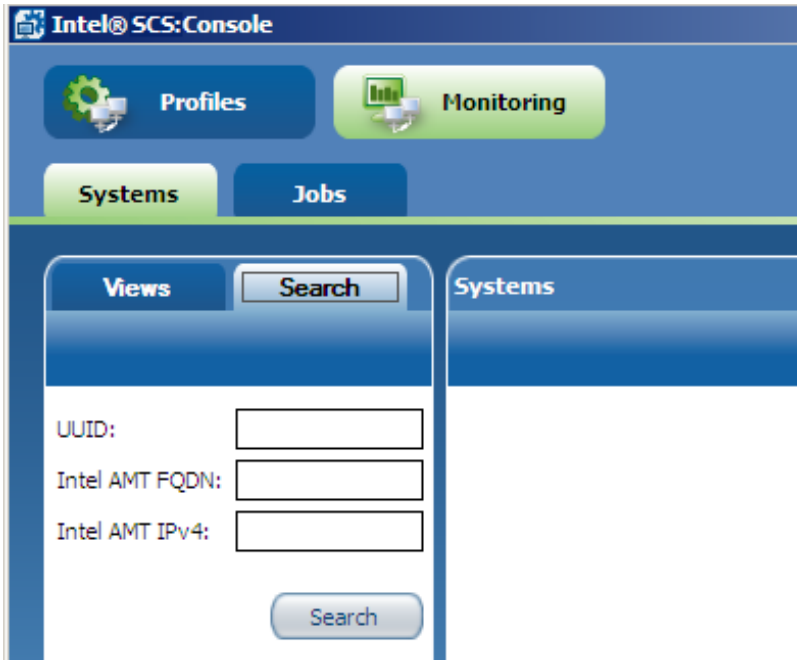


   Figure 7-4: Search Tab

2. In the available fields, enter the data that you want to use in the query

> **Note:**
>
> The query is constructed using these operators:
>
> - **Contains** – This means that in each field you can enter any part of the data that you have. For example, if you enter "555" in the UUID field the query will get data for all systems that have "555" as part of the UUID.
> - **And** – This means that if you enter values in more than one field the query only gets data of systems that have both those values.

3. Click **Search**. The systems that meet the query conditions are shown in the list of systems in the right pane. If the system you are searching for is not in the list, modify the query and click **Search**.

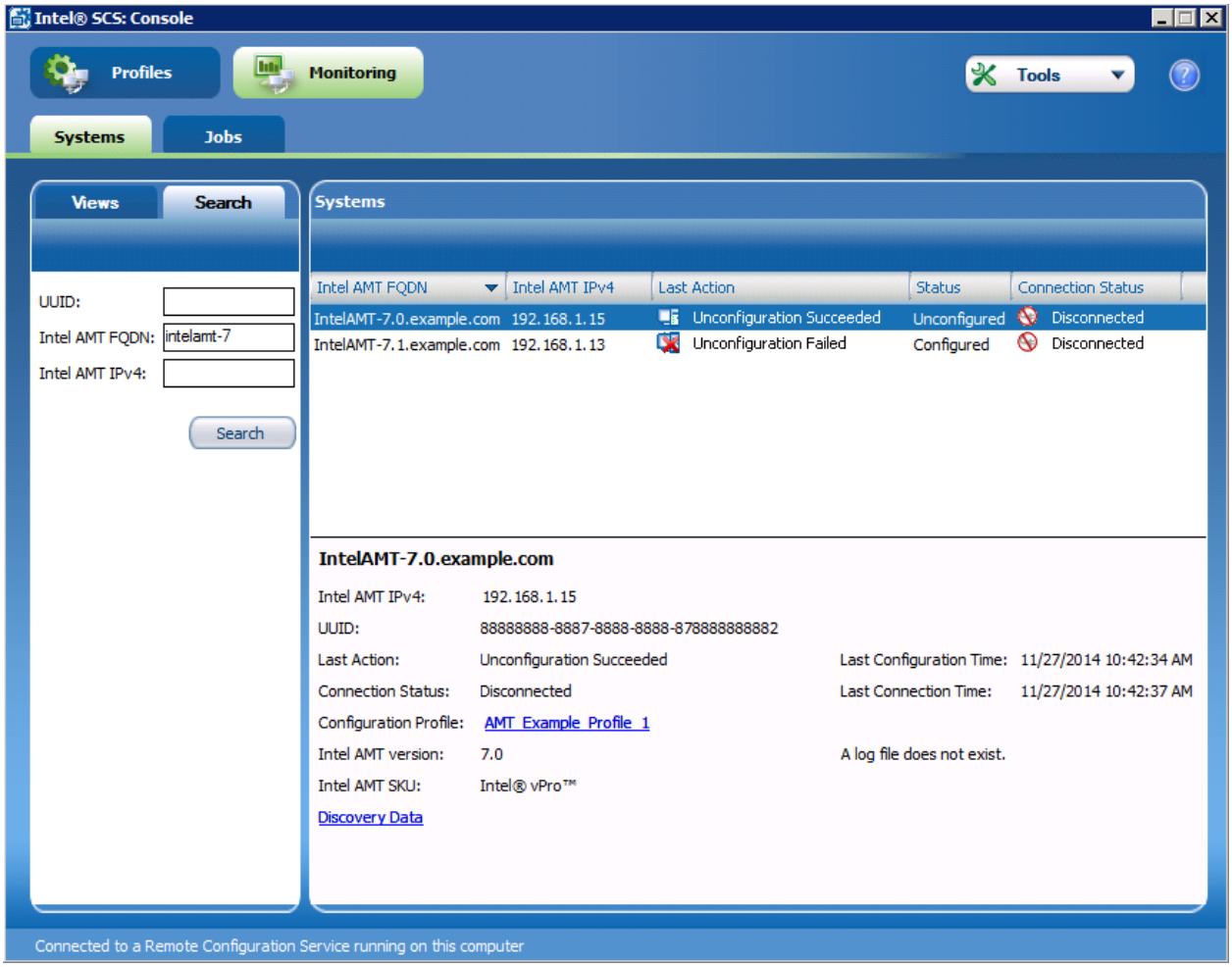


Figure 7-5: Example of Search Results

4. Click a system in the list. Data for the selected system is shown in the bottom section of the Systems pane. The profile that was used during the last configuration/reconfiguration operation is shown as a link. You can view the profile details by clicking the link.

   For information about other options available from the List of Systems, see:

   - Sorting the List of Systems on the next page
   - Getting the Admin Password on page 174
   - Viewing Operation Logs on page 175

   For a list of the possible statuses, see Last Action and Configuration Status on page 180.

7.6 Sorting the List of Systems

You can define which columns are shown in the list of systems by right-clicking the column header and selecting the columns. You can also sort the contents of the list by double-clicking a column header. You can do this for lists created using the Views tab and the Search tab. This table describes the available data.

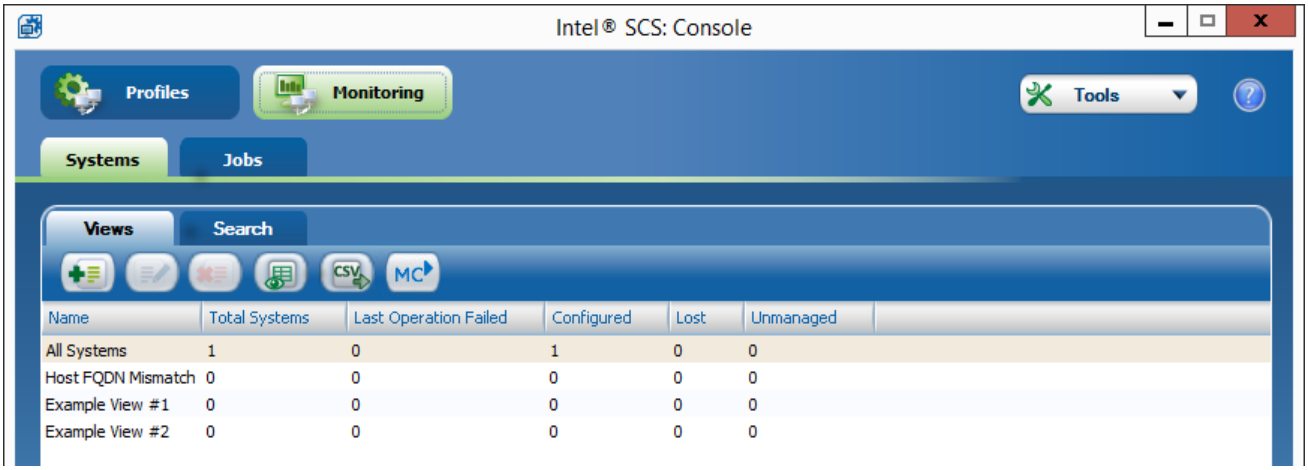
Table 7-2: Available Data

Column	Description
UUID	The Universally Unique Identifier of the Intel AMT device
Intel AMT FQDN	The FQDN defined in the Intel AMT device
Intel AMT IPv4	The IPv4 address of the wired LAN interface defined in the Intel AMT device
Last Action	See Last Action and Configuration Status on page 180
Status	
Version	The Intel AMT version
Profile	The profile that was used the last time that the Intel AMT system was configured
Active Directory OU	The Organizational Unit in Active Directory where the object representing the Intel AMT system is located
Sku	The Stock Keeping Unit
Connection Status	Defines if the RCS can connect to the Intel AMT device
Last Connection Time	The last date and time that the RCS successfully connected to the Intel AMT device
Last Configuration Time	The last date and time that the Intel AMT device was configured by the RCS
Managed State	See Changing the Managed State of Systems on page 171
Intel AMT FQDN	See Detecting and Fixing Host FQDN Mismatches on page 172

7.7 Exporting Profiles to CSV

To export the current list of profiles to a list of comma-separated values in a .csv file, click the Export to CSV button  .

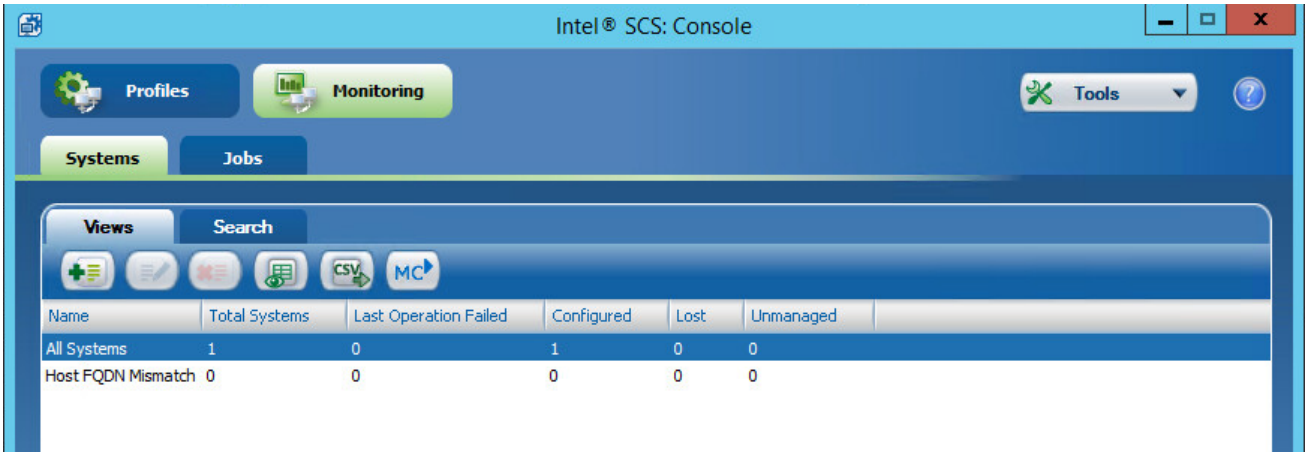
A Save As dialog box appears. Choose a location for the exported CSV file, type a name for it in the File name field, and click the Save Button. Your CSV file is saved in the specified file.



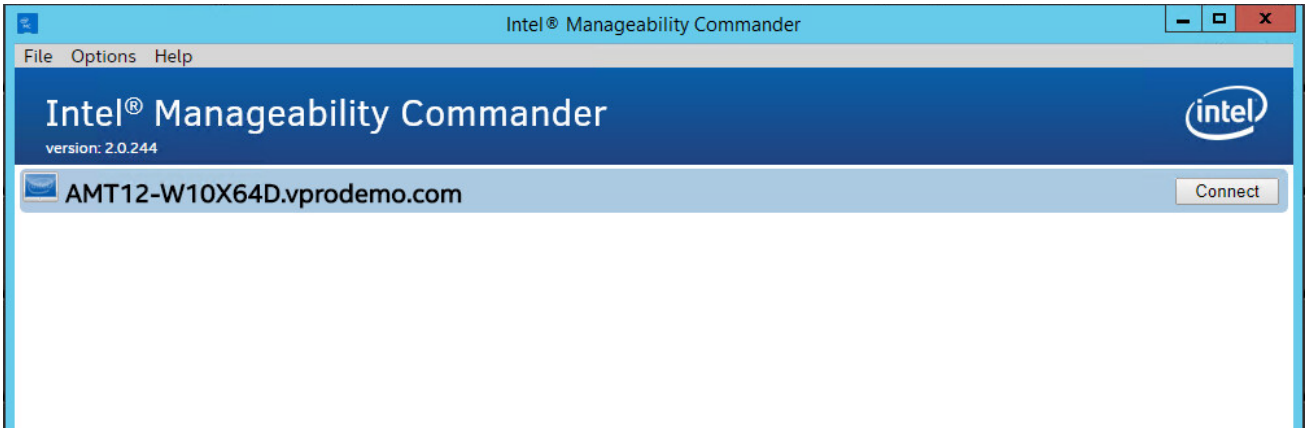
7.8 Viewing Systems Using the Intel® Manageability Commander Tool

The SCS Console allows you to manage systems using the Intel® Manageability Commander Tool (IMC) through a dedicated button.

To view systems in the IMC, click the MC button.



The Intel® Manageability Commander Tool appears, and loads the address information of the systems in the currently selected view in SCS.



When you click the MC button, the SCS console harvests the addresses of the systems belonging to the currently selected view, and serializes them into a connection file that is consumed by the IMC application, which assumes that the list of machines is configured with Kerberos ACL, and that the logged-on user is listed in the ACL configuration of the AMT platforms. The SCS console starts a new process for the IMC application using this connection file, simplifying the use of IMC with SCS.

The MC button is enabled only if the IMC application is installed in the platform hosting the SCS console. To locate the IMC installation directory, the SCS console queries the following registry key: **HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Intel\Intel Manageability Commander\Setup:installDir**

For more information on IMC and its usage, refer to the IMC User Guide or visit https://www.intel.com/content/www/us/en/support/software/manageability-products/intel-manageability-commander.html.

7.9 Changing the Managed State of Systems

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

- **Managed** – In this state, you can use all the options available from the Console
- **Unmanaged** – In this state, you can only view the system in the Console. You cannot include it in a job, get the password, or run data discovery from the Console. Before you can use the Console options, you must change the managed state of the system to Managed.

To change the management state:

1. In the Console, click **Monitoring** and select the **Systems** tab.
2. Locate the umanaged systems using the Views tab or the Search tab.

   Note:

   In the Views tab, umanaged systems are shown in the Unmanaged column. To view only these systems, right-click this column and select **Show Systems (this column only)**.

3. Select the system (or systems), right click, and select **Move to Managed State**.

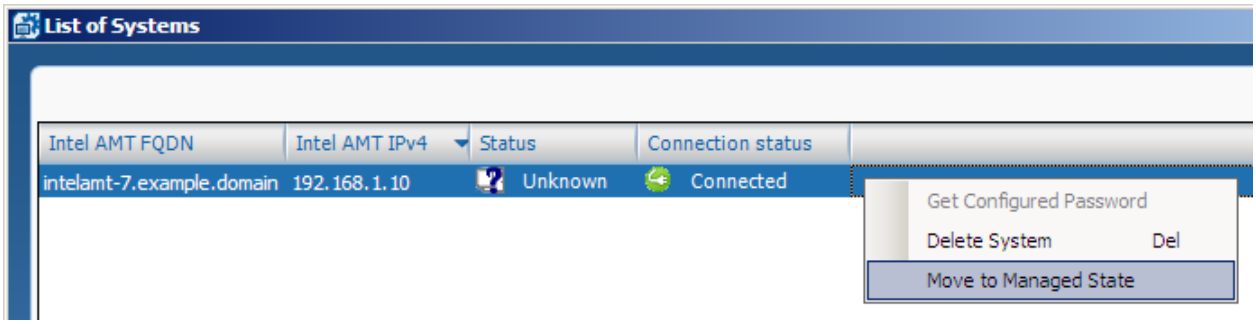


Figure 7-6: Move to Managed State Option

The systems are moved to the Managed state and you can use all the options available from the Console.

Note:

If the system is already in the Managed state, this menu option is not shown.

7.10 Detecting and Fixing Host FQDN Mismatches

The source used to configure the FQDN setting (hostname.suffix) in the Intel AMT device is defined in the configuration profile. The profile includes several options that you can use to define how the FQDN of the device will be constructed (see Defining IP and FQDN Settings on page 123).

When changes are made to the host computer or the network environment, the basis on which the FQDN setting was constructed might change. These changes can include changing the hard disk, replacing the operating system, or re-assigning the computer to a different user. If the FQDN setting in the Intel AMT device is not updated with these changes, problems can occur.

For example, many organizations use the name of the computer user as part of the hostname. When re-assigning a computer to a different user, they reconfigure the hostname in the operating system with the name of the new user. During support calls the support personnel use this hostname to locate and identify the computer in the network. If the FQDN setting of the Intel AMT device contains the old hostname, they might not be able to locate or connect to the correct device.

Intel SCS includes options that you can use to detect and fix these "mismatches".

Note:

The options described in this section are not available if you are using a dedicated network settings file to set the FQDN.

Viewing Host FQDN Mismatches

The **Monitoring** > **Views** tab includes a default view named "Host FQDN Mismatch". This view only includes systems in the database that match this filter:

- Managed State = Managed
- Host FQDN State = Mismatch

For each system in the database, the Host FQDN State can be one of these values:

- **Unknown** – This is the value of all systems when they are first added to the database, or after a mismatch was fixed. These systems will remain in this state until discovery data is sent from the Configurator. When the discovery data is updated, the system will be moved to the Synchronized or the Mismatch state.
- **Synchronized** – The FQDN setting in the device and the profile are the same.
- **Mismatch** – The FQDN setting in the device does NOT match the FQDN setting currently defined in the profile associated with that system. These systems will remain in this state until the mismatch is "fixed". After the mismatch is fixed, the system will be moved to the Unknown state.

Note:

Even if mismatches exist, the Host FQDN Mismatch view will remain empty until you send discovery data from the Configurator. To do this, see Detecting Host FQDN Mismatches on the next page.

Detecting Host FQDN Mismatches

Host FQDN mismatches are detected using the `/ReportToRCS` parameter of the Configurator CLI `SystemDiscovery` command. For example:

```
ACUConfig.exe SystemDiscovery /ReportToRCS /AdminPassword <password> /RCSAddress <RCSAddress>
```

For the full syntax of this command, see Discovering Systems on page 129.

This is what occurs (for each system) when you use this parameter:

1. The discovery data is sent to the RCS and added/updated in the record of the Intel AMT system in the database. This data includes all the network related settings that are currently defined in the host operating system and the Intel AMT device. You can view this data in the Host Based tab of the Discovery Data window (in the "Intel AMT" entry).
2. The RCS uses the discovery data to compare the FQDN setting in the device with the FQDN setting defined in the profile.
3. The RCS updates the value of the Host FQDN State property of the system:
   - **Synchronized** – If the settings match.
   - **Mismatch** – If the settings do not match. These systems are shown in the Host FQDN Mismatch view (see Viewing Host FQDN Mismatches on the previous page).

> **Note:**
>
> - New mismatches can occur at any time. The RCS is only updated with new mismatches when you run the `SystemDiscovery` command with the `/ReportToRCS` parameter. Thus it is recommended to run this command and parameter at regular intervals.
> - For information about how to fix the mismatches, see Fixing Host FQDN Mismatches below.

Fixing Host FQDN Mismatches

Host FQDN mismatches are fixed using jobs.

To fix host FQDN mismatches using a job:

1. Create a job. In the Job Definition window, select these options:
   - From the drop-down list in the Filter section, select **Host FQDN Mismatch**.
   - From the Operation drop-down list, select **Fix host FQDN mismatch**.

     > **Note:**
     >
     > - Fix host FQDN mismatch is the only job operation type that can always correctly fix Host FQDN mismatches.
     > - You can create a recurring job that will automatically run and fix mismatches on any systems that are added to the Host FQDN Mismatch view.

2. Complete the rest of the job definitions that you want to define for this job (see Creating a Job on page 186).

3. When the job runs, the RCS tries to configure the correct FQDN in each Intel AMT device. When a mismatch is fixed, the Host FQDN State of the system is changed to Unknown.
4. When the job is in the Completed status (see Job Statuses on page 186), make sure that the mismatches were fixed. You can do this by opening the List of Systems in Job window (see Viewing Job Items on page 188). Each system with a Status of "Completed Successfully" will no longer be included in the Host FQDN Mismatch view.
5. Update the discovery data of these systems so that the RCS can change the Host FQDN State of the system to Synchronized (see Detecting Host FQDN Mismatches on the previous page).

7.11 Getting the Admin Password

In database mode, you can use the Console to send a query via the RCS to verify the Digest admin password defined in the Intel AMT device. The RCS tries to connect to the device using the password defined in the database for the selected system. If this fails, the RCS tries the admin passwords defined in the configuration profiles. If a Digest Master Password file exists, the RCS will also try the passwords that the file contains. If connection is successful, the RCS shows the password and updates the password in the database if necessary.

To get the Admin password:

1. In the Console, click **Monitoring** and select the **Systems** tab.
2. Locate and select the system using the Views tab or the Search tab. Data for the selected system is shown in the bottom section of the window.
3. Right-click the system and select **Get Configured Password**. The View System's Password window opens.

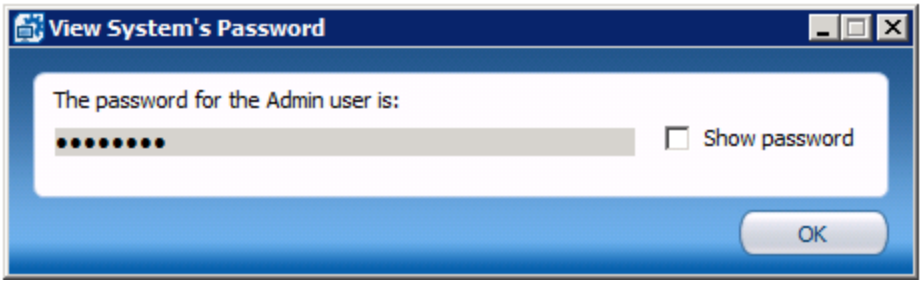


Figure 7-7: View System's Password Window

4. To view the password, select **Show password**. The password is shown.

7.12 Viewing Operation Logs

Data about each operation that the RCS does on a system is stored in the database. Two records are created for each operation:

- **Start Record** – This record is created when the operation starts and contains the word "Start" in the name of the operation. The description field of this record contains a list of the parameters that were used during the operation. You can use this data to troubleshoot what happened if problems have occurred.
- **Finish Record** – This record is created when the operation finishes. The description field of this record shows details of problems that occurred. For these records, the Severity level column can show one of these:
  - Success – The operation completed successfully
  - Completed with warnings – The operation completed, but some errors occurred. For configuration/reconfiguration operations, this means that the system was configured, but not all settings were set successfully.
  - Error – The operation failed

To view operation logs of a system:

1. In the Console, click **Monitoring** and select the **Systems** tab.
2. Locate and select the system using the Views tab or the Search tab. Data for the selected system is shown in the bottom section of the window.

> **Note:**
>
> You can also view the logs in the List of Systems in Job window (see Viewing Job Items on page 188).

3. Click **View Log**. The Operation Logs window opens.

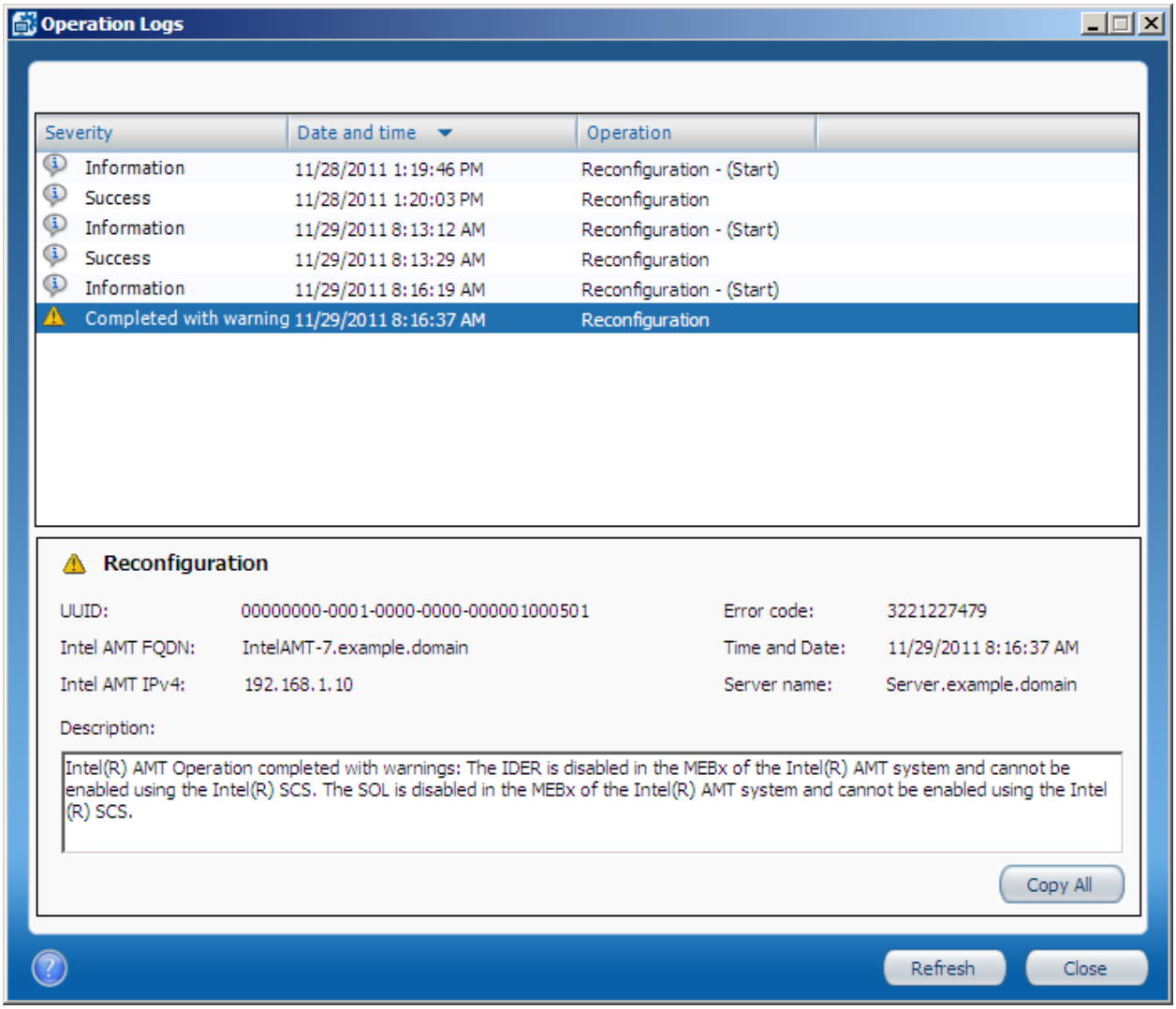


Figure 7-8: Operation Logs Window

Note:

Clicking **Copy All** copies the data for the selected record to the clipboard. You can then paste the data (Ctrl + V) to a text editor.

7.13 Viewing Discovery Data

The Discovery Data window lets you view data collected by the Configurator and the RCS. For more information about the discovery options, see What are the Discovery Options? on page 3.

Note:

The data collected by the Configurator and the RCS is stored separately in the database for each system. This means that there can be duplicate data for the same system, and even contradicting data. The last date and time that each of the Intel SCS components got data from the system is shown in the Console.

To view discovery data of a single system:

1. In the Console, click **Monitoring** and select the **Systems** tab.
2. Locate and select the system using the Views tab or the Search tab. Data for the selected system is shown in the bottom section of the window.

   Note:

   You can also view the discovery data in the List of Systems in Job window (see Viewing Job Items on page 188).

3. Click **Discovery Data**. The Discovery Data window opens.

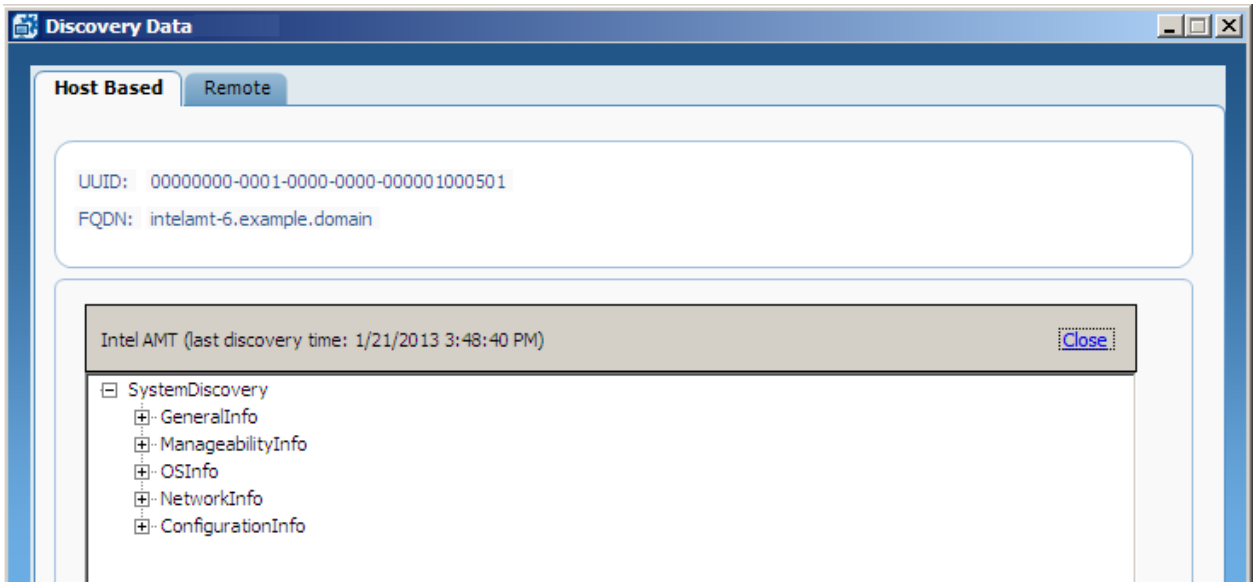


Figure 7-9: Discovery Data Window

The Discovery Data window includes two tabs:

- **Host Based** – This tab contains data collected locally on the system and sent to the RCS. If data exists, click **Expand** to show the data. In the tree view, expand the nodes to see the data that they contain.
- **Remote** – Contains data collected (remotely) by the RCS.

4. To view/get remote discovery data, select the **Remote** tab. The Remote tab opens.

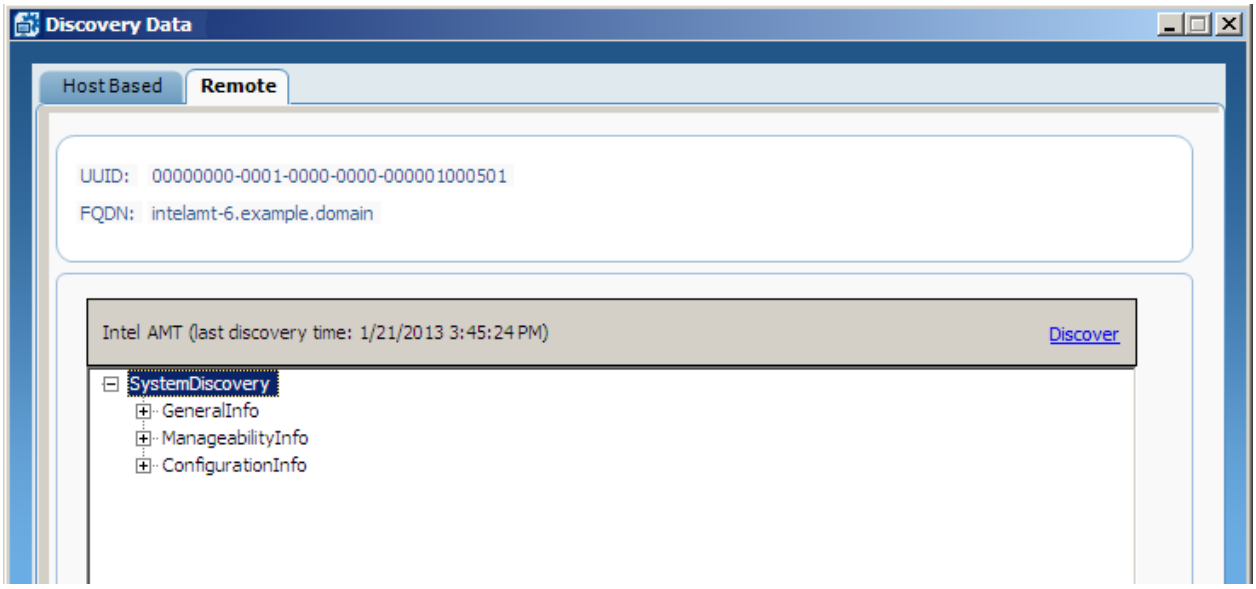


Figure 7-10: Remote Tab

5. If data does not exist, click **Discover** to send a new query to the system (via the RCS) and update the database. When the query has completed, the data is shown in a tree view. You can expand the nodes to see the data that they contain. Each time that you click Discover, a new query is sent to the system.

To get data for multiple systems:

1. In the Console, create a job (see Creating a Job on page 186).
2. When you create the job, select the **Get discovery data** option from the Operation drop-down list.
3. After you run the job, you can also view the discovery data of each system in the List of Systems in Job window (see Viewing Job Items on page 188).

7.14 Last Action and Configuration Status

When viewing lists of systems, you can see the configuration status of each system in the Status column:

- **Configured** – The system is configured
- **Unconfigured** – The system is unconfigured
- **Unknown** – The RCS does not know the status of the system

> **Note:**
>
> The state shown in the Status column will not always be 100% accurate The value assigned to each system can only reflect the configuration status as known by the RCS.

In addition, the Last Action column shows information about the last action that was performed on the system by the RCS:

- **Configuration Succeeded** – The system was configured successfully
- **Configuration Failed** – The RCS failed to configure the system
- **Configuration Update Failed** – The RCS failed to perform a configuration update (reconfiguration) on the system
- **Maintenance Succeeded** – Maintenance tasks run by the RCS completed successfully
- **Maintenance Failed** – One or more of the maintenance tasks run by the RCS failed
- **Connection Check Failed** – The post configuration connection check (performed by the RCS) failed to connect to the Intel AMT device
- **Configuration Script Failed** – A post configuration script, run by the RCS, failed or returned an error
- **Unconfiguration Failed** – The RCS failed to unconfigure the system
- **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
- **Unconfiguration Succeeded** – The system was unconfigured successfully by the RCS
- **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 RCS does not know the status of the last action performed on the system

Chapter 8

Managing Jobs and Operations

This chapter describes how to use the jobs options, available from the Console, when working in database mode.

> **Note:**
>
> You can only use these options on systems that exist in the database and are in the Managed state.

For more information, see:

8.1 About Jobs and Operations

A "job" is an operation that you can run from the Console on a selected group of Intel AMT systems, defined using a filter.

The **Monitoring** > **Jobs** tab shows a summary of all existing jobs.

Figure 8-1: Example of Jobs

Note:

For more information about the data available from the list of jobs, see Viewing the List of Jobs on the next page.

This table describes the options available from the Jobs tab.

Table 8-1: Jobs Tab Options

Click	To do this...
	Create a new job (see Creating a Job on page 186)
	Edit the job selected in the list. You can only edit a job if it is in the "Waiting" or "Scheduled" status. **Note:** You can only edit some of the fields in the job.
	Delete the job(s) selected in the list.You can only delete a job if it is in a status of "Scheduled", "Waiting", "Completed", or "Aborted".
	View the systems in a job (see Viewing Job Items on page 188)
	Start a manual job selected in the list (see Starting, Aborting, and Deleting Jobs on page 190)
	Abort the job selected in the list

8.2 Viewing the List of Jobs

The number of systems in a job and the status of the systems is shown in the columns of the jobs list. These columns are automatically updated to show the current status of the job and the systems. You can show/hide columns by right-clicking the column header and selecting the columns that you want to show.

Table 8-2: Available Data in the Jobs List

Column	Description
Name	The name you defined for the job
Description	The optional description you defined for the job
Operation	The type of operation (see Job Operation Types on the next page)
Status	The status of the job (see Job Statuses on page 186)
All Systems	The total number of systems defined in the job
Succeeded	The number of systems on which the operation completed
Succeeded with Warnings	The number of systems on which the operation completed, but with warnings
Failed	The number of systems on which the operation failed
Waiting for Retry	The number of systems on which the operation could not run, and the RCS is waiting to retry the operation. The RCS includes an automatic retry mechanism for job operations: • Retry 5 times, each after a pause of 1 minute • Then retry 5 more times, each after a pause of 1 hour • Then retry 5 more times, each after a pause of 24 hours After 15 unsuccessful retry attempts, the system is added to the total number of systems in the Failed column.
In Operation	The number of systems on which the job is currently running
Aborted	The number of systems on which the operation was not run because the job was aborted

8.3 Job Operation Types

The operation that you define in a job is run on all systems that are defined in the job. You can define only one operation per job. These are the available types of operation:

Configuration

This operation reconfigures the systems with the settings defined in the profile that you select from the drop-down list.

Note:

- If the Network Settings (IP and FQDN) were changed in the profile, this operation type will NOT make those changes in the device. This is because the RCS cannot get the necessary information from the host operating system. If you need to reconfigure a device with new network settings, use the configuration commands available from the Configurator.
- In certain conditions, this operation might fail on unconfigured systems (see Configuration via Jobs Fails because of OTP Setting).

Full Unconfiguration

This operation deletes all the Intel AMT setup and configuration settings from the systems and disables the Intel AMT features on the systems.

Note:

This operation type also deletes customized data. For example:

- Any root certificate hashes that were entered manually into the Intel MEBX
- Any customized data that was pre-defined by the manufacturer (for example, the PKI DNS Suffix).

Do not use this operation type if your configuration flow relies on customized data. (For example, remote configuration of LAN-less systems into Admin Control mode requires a pre-defined customized value in the PKI DNS Suffix.)

Partial Unconfiguration

This operation removes the configuration settings from the systems and disables the Intel AMT features on the systems. The systems and the RCS can still communicate since the PID, PPS, admin ACL settings, host name, domain name, and the RCS IP and port number are not deleted.

Note:

- If the OEM defined the SOL and IDE interfaces to be closed by default, then unconfiguration operations will close them and they cannot be reopened without physical access to the Intel MEBX. This is a known Firmware limitation.
- If auditing was enabled on the Intel AMT system, you cannot run unconfiguration operations unless it is permitted by the auditor.

Maintenance

This operation runs maintenance tasks on the systems:

- **Synchronize the clock** – Synchronizes the clock in the Intel AMT device with the clock of the computer running the RCS. This task is always performed.
- **Renew the Digest Admin password** – Renews the password of the Digest admin user according to the password setting defined in the profile. This task is always performed.
- **Re-issue certificates** – Re-issues PKI certificates that are close to the expiry date. This task is only run if you select the check box.
- **Renew AD password** – Changes the passwords of the ADOU objects representing the Intel AMT systems. This task is only run if you select the check box.

Note:

For some of these tasks, the RCS needs data stored in the configuration profile. By default, the RCS uses the configuration data that was last used to configure the system stored in the database. If you select a different profile from the drop-down list, the data from the selected profile is used instead. This applies to Operations Maintenance and Automatic Maintenance.

Automatic Maintenance

This operation runs the maintenance tasks (described in the Maintenance operation) on the systems only if they are necessary. This is possible because Intel SCS saves some configuration related data in the database record of each Intel AMT system. The database record is updated each time that a job is run on the system.

When you use the Automatic Maintenance operation:

1. The RCS uses the data in the database to make the decision which maintenance tasks are necessary for each Intel AMT system:
   - **Synchronize the clock** – If not synchronized for more than three months
   - **Renew the Digest Admin password** – If the last renewal of the Digest Admin password was more than six months ago
   - **Re-issue certificates** – If there are less than 30 days before one of the certificate expiration dates
   - **Renew AD password** – If the last renewal of the ADOU object password was more than six months ago
2. The RCS automatically does only the necessary tasks that were identified in step 1. If no tasks are necessary, nothing is done.

Get Discovery Data

This operation gets Intel AMT related data from the systems (see Viewing Discovery Data on page 177).

Fix Host FQDN Mismatch

This operation fixes Host FQDN Mismatches (see Detecting and Fixing Host FQDN Mismatches on page 172).

8.4 Job Statuses

A job can be in one of these statuses (shown in the Status column of the list of jobs):

- **Scheduled** – The job was defined to start automatically at a specific date and time in the future. Jobs in this status can also be recurring jobs that will automatically run according to an interval (of days) that you define.
- **Preparing Job** – A manual job was created and the RCS is currently preparing the list of systems on which the job will run. When complete, the status of the job will change to "Waiting".
- **Waiting** – The job has not started yet. This is the status of all new manual jobs until you start the job (see Starting, Aborting, and Deleting Jobs on page 190).
- **In Progress** – The job has started to run. The job will stay in this status until the operation has run on all systems, or the job is aborted.
- **Completed** – The job was run on all systems. This does not mean that the job was successful on all the systems. (The other columns in the list of jobs show the status summary.) This status is only relevant for non-recurring jobs. After a recurring job has completed, the status of the job will change to Scheduled.
- **Aborting** – The job was aborted, but the operation is still running on the systems where it had already started to run before the job was aborted. After the operation has run on all systems where it is already running:
  - For non-recurring jobs, the status of the job will change to Aborted.
  - For recurring jobs, the status of the job will change to Scheduled.
- **Aborted** – The job was aborted and the operation has run on all the systems where it had already started to run before the job was aborted.

8.5 Creating a Job

You can create two types of jobs:

- **Manual** – This type of job only runs once, and must be started manually.
- **Automatic** – This type of job is automatically started by the RCS at the time and date that you specify in the job. You can define this type of job to run once, or at specified intervals (a "recurring" job).

To create a job:

1. In the Console, click **Monitoring**.
2. Select the **Jobs** tab and click  . The Job Definition window opens.

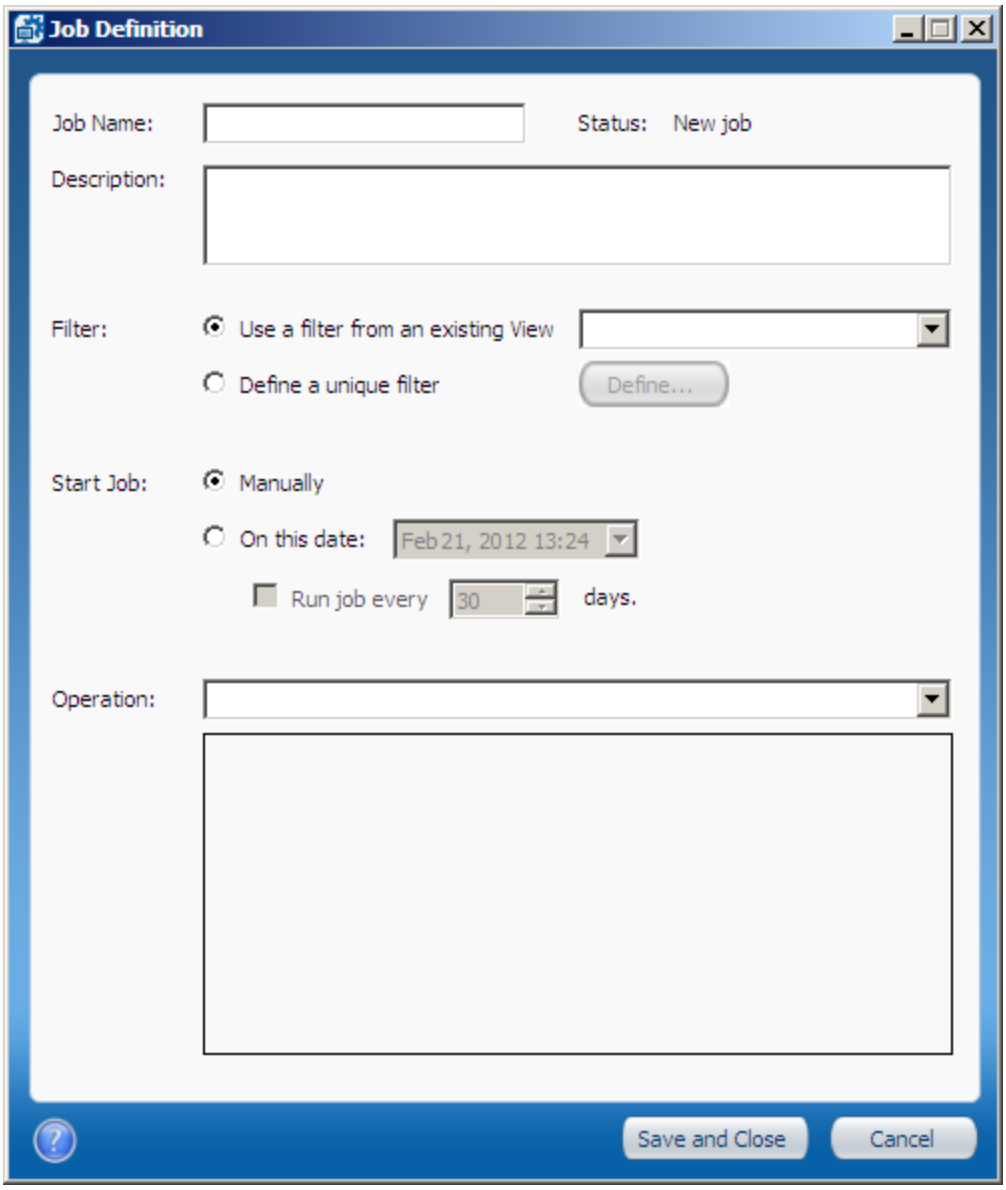


Figure 8-2: Job Definition Window

3. In the Job Name field, enter a name for this job.
4. (Optional) In the Description field, enter a description for this job. This field is for informational purposes only.

5. In the Filter section, define on which systems this job will run:
   - **Use a filter from an existing View** – Select this option to use a filter from an existing view. Select the view from the drop-down list.
   - **Define a unique filter** – Select this option to define a filter that will be used in this job only. Click **Define** to define the filter (see Defining a System Filter on page 163).
6. In the Start Job section, select when the job will start:
   - **Manually** – Select this option to define a manual job. This type of job must be started manually (see Starting, Aborting, and Deleting Jobs on page 190).
   - **On this date** – Select this option to define an automatic job. By default, today's date is selected. You can edit the date and time directly in the field, or open a calendar to select a different date. If you want to define a recurring job, select the **Run job every** check box and define the number of days for the interval. The interval can be a minimum of 7 days and a maximum of 365 days.

     Note:

     After a recurring job completes, the date defined in the job for the next run is automatically updated. You can also manually change the date, time, and interval of automatic jobs (but only when the status of the job is "Scheduled").
7. From the Operation drop-down list, select the type of operation that this job will perform (see Job Operation Types on page 184).
8. Click **Save and Close**. The Job Definition window closes and the job is added to the list of jobs.

8.6 Viewing Job Items

The systems that match the filter defined in the job are shown in the List of Systems in Job window. These "job items" are the systems on which the job will run.

You can view this list and get data about the systems in the list.

Note:

- For manual jobs, this list only includes systems that matched the filter at the time that the job was created. If more systems are added to the network that match the filter, they will NOT be added to the job.
- For automatic jobs, the systems are added to the list just before the job starts. This means that the job will run on systems that match the filter at the time that the job starts.
- For recurring jobs, the list of systems in the job is automatically updated each time the job starts.

To view the job items:

1. In the Console, click **Monitoring** and select the **Jobs** tab.
2. Right-click the job and select **View Systems**. The List of Systems in Job window opens.

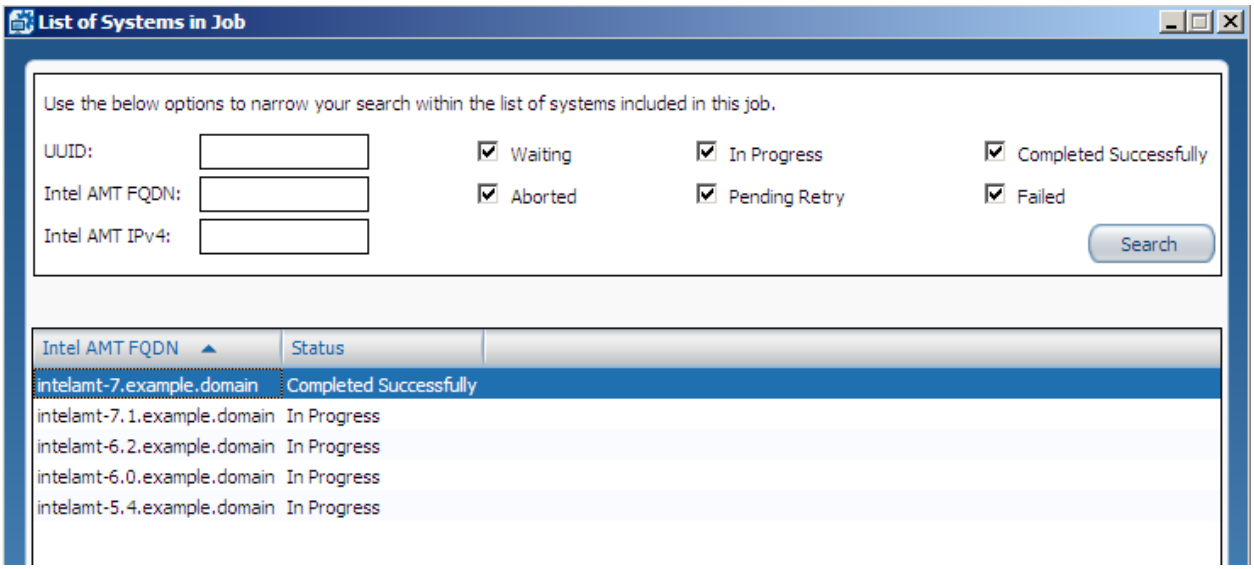


Figure 8-3: List of Systems in Job Window

Note:

- You can show/hide systems in the list using the check boxes and the search fields columns and then clicking **Search**.
- If the job status is "Waiting", you can delete systems from the list by right-clicking them and selecting Delete Item from List. If a system is deleted, the operation will not run on that system when the job starts. After a job starts, you cannot delete a system from the job.
- You can view the operation logs of a system by selecting the system and clicking **View logs**. For more information about logs, see Viewing Operation Logs on page 175.

8.7 Starting, Aborting, and Deleting Jobs

Automatic jobs are started automatically by the RCS.

Manual jobs must be started from the Console.

When a job is in the "Completed" or "Scheduled" status, you can delete the job.

To start a manual job:

In the list of jobs:

- Right-click the job and select **Start Job**.

- Or -

- Select the job and click  .

To delete a job:

- In the list of jobs, select the job and click  .

About aborting a job

At any time after a job has started, you can abort the job. To do this, in the list of jobs:

- Right-click the job and select Abort Job.

- Or -

- Select the job and click  .

When a job starts, the RCS starts the operation simultaneously on the first 50 systems defined in the job. After 30 seconds, the RCS starts the operation on another set of systems (up to the maximum of 50 systems). This cycle continues until the operation is run on all systems in the job.

Note:

At any time after creating a job, you can check the status of the operation on each system (see Viewing Job Items on page 188).

If you abort a job, the status of the job is changed to "Aborting". Operations that have already started on a system will not be aborted. When the operation has run on those systems, the status of the job is changed to "Aborted" (or "Scheduled" if the job is a recurring job). If an operation is in the "Pending Retry" status, aborting the job will cancel the operation on those systems.

Chapter 9

Preparing the Certification Authority

This chapter describes the prerequisites and procedures for using a Certification Authority (CA) with Intel SCS.

For more information, see:

9.1 About Certification Authorities

A certificate authority (CA) is necessary if you want to configure any of these settings in an Intel AMT device:

- Remote Access
- Transport Layer Security
- 802.1x Setups
- End-Point Access Control

During configuration of these settings, Intel SCS sends a request to a CA software application to generate a certificate. Intel SCS puts the generated certificate in the Intel AMT device. Intel SCS can request certificates

- From a Microsoft* CA – This is the default option, and is described in Using Intel SCS with a Microsoft CA below. For information on installing a Microsoft CA, see Microsoft's documentation.
- Via a CA Plugin – This option is only available after a plugin is installed.

9.2 Using Intel SCS with a Microsoft CA

This section describes the prerequisites necessary to use Intel SCS with a Microsoft CA.

See the Intel AMT documentation on Certificate Management for more details.

9.2.1 Standalone or Enterprise CA

Intel SCS supports the Standalone and Enterprise versions of Microsoft CA. An Enterprise CA can be configured only in conjunction with Active Directory. A Standalone CA can operate with or without Active Directory. (If Active Directory is not present, there can be only one RCS instance and the Standalone CA must be installed on the same server as the RCS.) The Microsoft CA can have a hierarchy of CAs, with subordinate CAs and a root CA. This is beyond the scope of this guide.

These features require a Standalone root CA or an Enterprise root CA:

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

These features require an Enterprise root CA:

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

9.2.2 Defining Enterprise CA Templates

If you use Intel SCS with an Enterprise CA and configure Intel AMT features to use certificate-based authentication, you must define certificate templates.

Note:

This procedure shows how to create a template containing the correct settings for Intel AMT. For settings specific to your organization (such as certificate expiration), specify the values you require. You must also make sure that the CA and the template are not defined to put certificate requests into the pending status. For more information, see Request Handling on page 198.

To create a certificate template:

1. From your Certificate Authority server, select **Start** > **Run**. The Run window opens.
2. Enter **mmc** and click **OK**. The Microsoft Management Console window opens.
3. If the Certificate Templates plug-in is not installed, perform these steps:
   a. Select **File** > **Add/Remove Snap-in**. The Add or Remove Snap-ins dialog box appears.
   b. From the list of available snap-ins, select **Certificate Templates**, click **Add** and then click **OK**. The Add or Remove Snap-ins dialog box 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 is shown in the right pane.

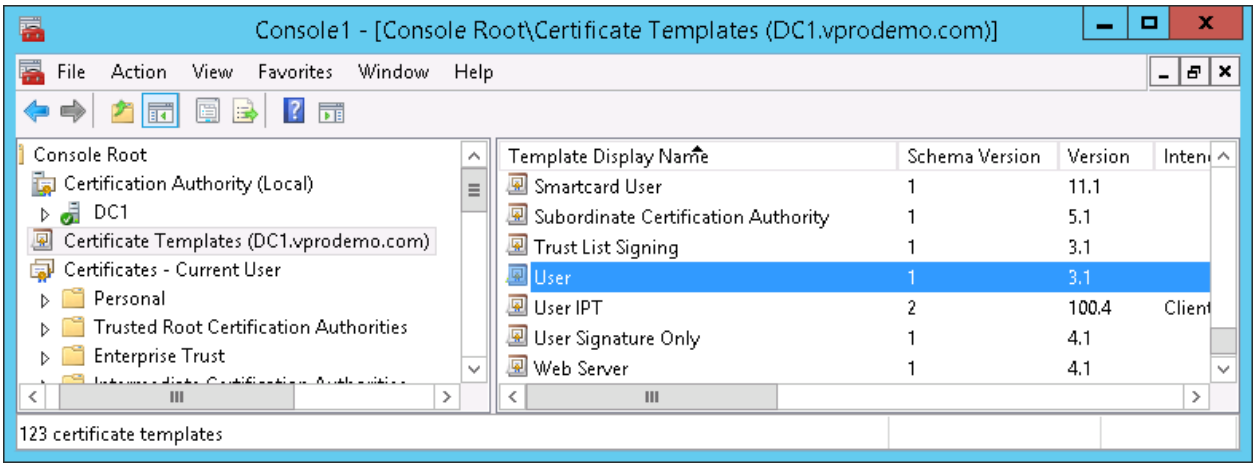


Figure 9-1: Microsoft Management Console

5. In the right-pane, right-click the **User** template and select **Duplicate Template**. The Properties of New Template dialog box appears, showing the **Compatibility** tab.

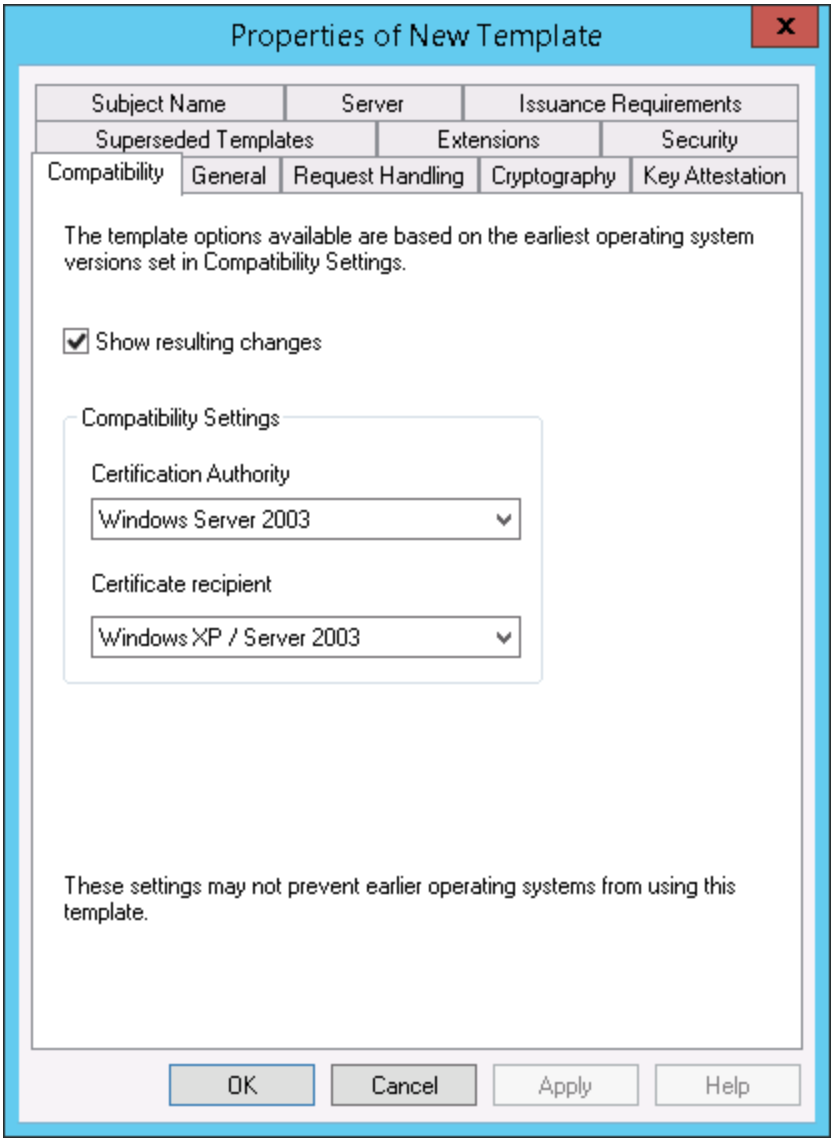


Figure 9-2: Properties of New Template dialog box, Compatibility tab

Note:

Intel SCS supports version 1, 2, 3, and 4 certificate templates.

6. Make sure that you select an appropriate combination of **Certification Authority** and **Certificate recipient** compatibility settings, as shown in the following table:

Certification Authority	Certificate Recipient
Windows Server 2012*	Windows 8* / Windows Server 2012
Windows Server 2012	Windows 8.1* / Windows Server 2012 R2
Windows Server 2012 R2*	Windows 8 / Windows Server 2012
Windows Server 2012 R2	Windows 8.1 / Windows Server 2012 R2
Windows Server 2016*	Windows 10* / Windows Server 2016

If **Show resulting changes** is selected, as you change the combination of **Certification Authority** and **Certificate recipient** settings, A Resulting changes dialog box may appear, listing the template options that will be removed with the given settings. Click **OK** to accept these changes.

The settings that you configure on the Compatibility tab and in the certificate template properties determine the certificate template schema version that is created when the template is saved. The logic for determining the certificate template schema version that is created is as follows:

- If the CA operating system is Windows Server 2012 and the certificate recipient operating system is Windows 8, then a version 4 certificate template schema version is created.
- If the CA operating system is earlier than Windows Server 2012 or the certificate recipient is earlier than Windows 8, then a certificate template schema version 4 template is not created. The type of template created depends upon the cryptographic provider that is selected:
  - If a cryptographic service provider (CSP) is selected, then a certificate template schema version 2 is created
  - If a key storage provider (KSP) is selected, then a certificate template schema version 3 is created.

For more information, see https://social.technet.microsoft.com/wiki/contents/articles/13303.windows-server-2012-certificate-template-versions-and-options.aspx.

7. Next, click the **General** tab. On this tab, make sure that the **Publish certificate in Active Directory** check box (highlighted in red in Properties of New Template Window, General tab below) is NOT selected.

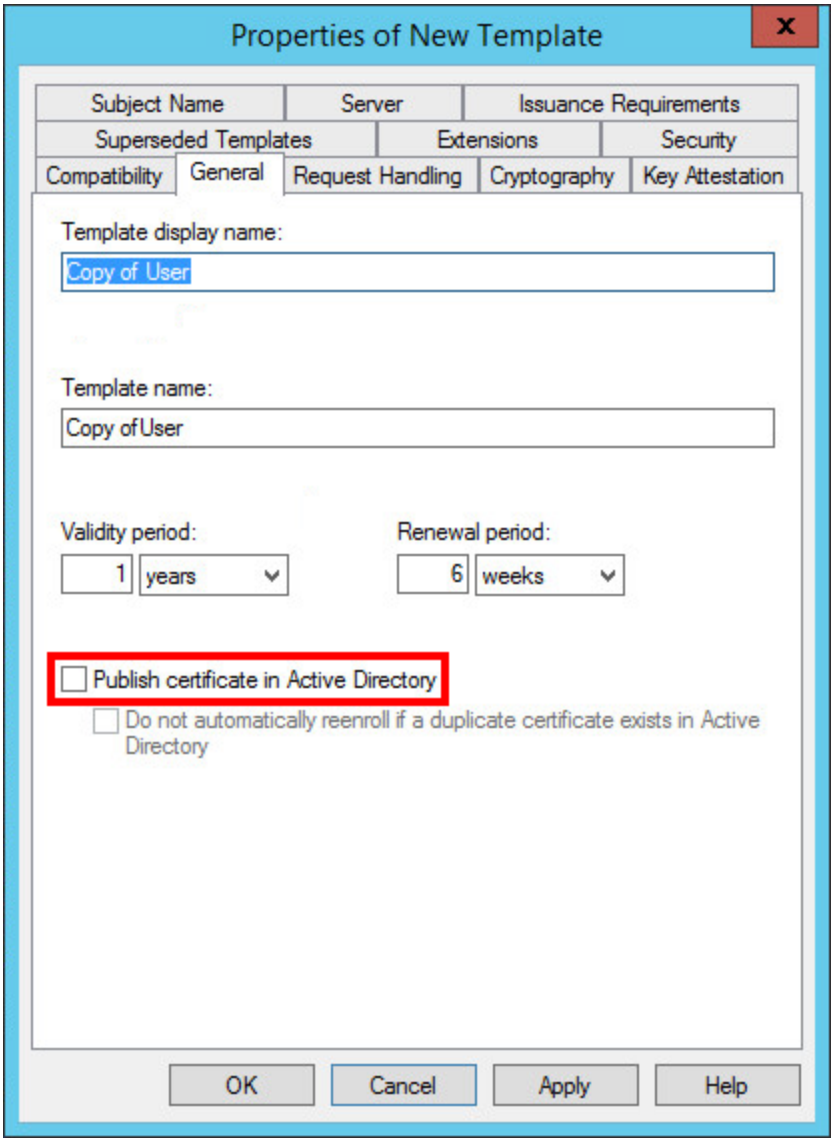


Figure 9-3: Properties of New Template Window, General tab

8. In the Template display name field, enter a meaningful name. For example, name a template used to generate 802.1x client certificates "802.1x".
9. Change the validity and renewal periods as required by local policy and click **Apply**.

10. Click the **Cryptography** tab.

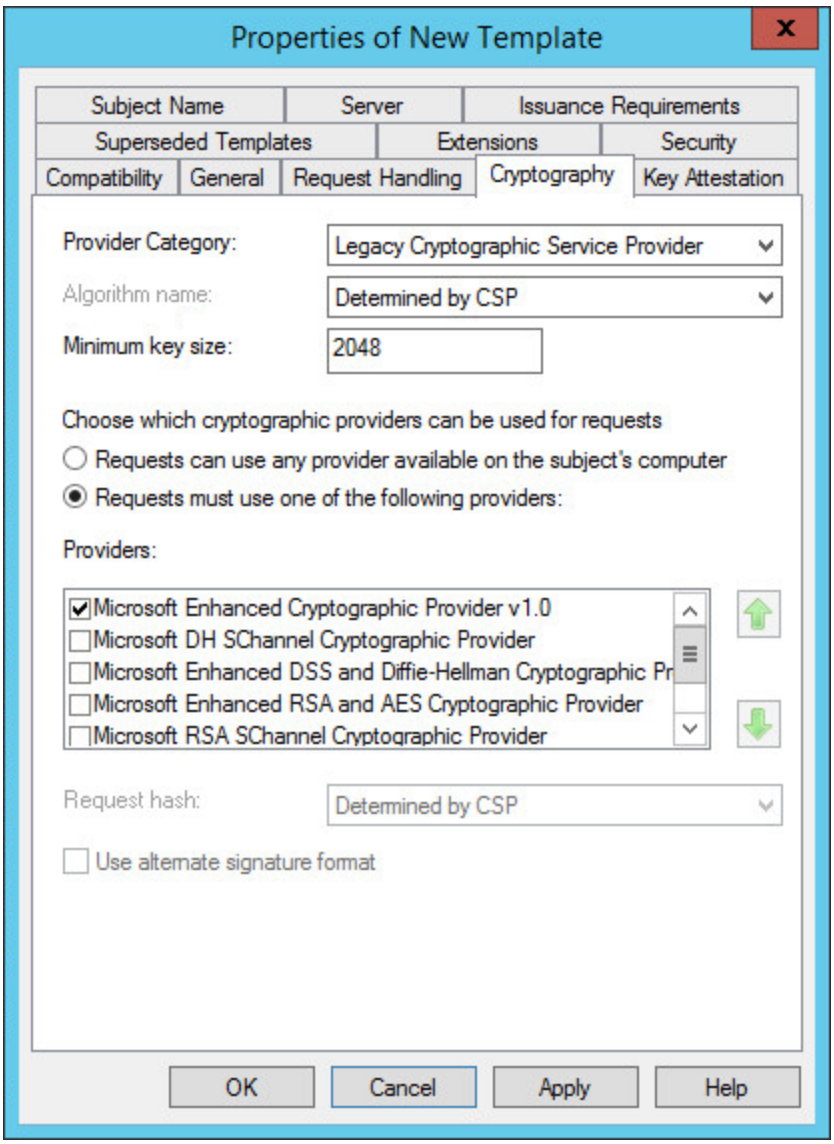


Figure 9-4: Properties of New Template Window, Cryptography tab

> **Note:**
>
> In the **Minimum key size** field, do not define a value higher than 2048. The maximum key size supported by Intel SCS is 2048. A minimum key size of 1024 is vulnerable, so not recommended.

11. In the **Providers** list, select the **Microsoft Strong Cryptographic Provider** check box and click **Apply**.
12. Click the **Subject Name** tab and select **Supply in the request**.
13. Click the **Security** tab. On this tab, make sure that the user running the Configurator (or the group the user is in) is included in the list of users and has the Read and Enroll permissions.

14. If this is a template for TLS, do these steps:

    a. Click the **Extensions** tab.

    b. From the list of extensions, select **Application Policies** and click **Edit**. The Edit Application Policies Extension dialog box appears.

    c. Click **Add**. The Add Application Policy dialog box appears.

    d. From the list of Application policies, select **Server Authentication** and click **OK**. (The Server Authentication policy contains this OID: **1.3.6.1.5.5.7.3.1**).

    e. Click **OK** to return to the Properties of New Template window.

    > **Note:**
    >
    > If you define Mutual TLS in the configuration profile, each application that needs to communicate with the Intel AMT device will need a certificate. In addition to the Server Authentication OID (added in step 15 d), the certificate must contain these OIDs:
    >
    > - For remote access: **2.16.840.1.113741.1.2.1**
    > - For local access: **2.16.840.1.113741.1.2.2**
    >
    > You can add these OIDs to this template (by clicking **New** in the Add Application Policy window). You must then install a certificate, based on this template, in the certificate store of the user running the application.

15. Click **OK**. The Properties of New Template window closes.
16. From the **Start** menu, select **Administrative Tools**. The Administrative Tools control panel appears. In the list of administrative tools, find **Certification Authority**, and double-click it. The Certification Authority
17. From the Console Root tree in the left pane, select **Certificate Templates**.
18. Right-click in the right pane and select **New** > **Certificate Template to Issue**. The Enable Certificate Templates dialog box appears.
19. Select the template that you just created and click **OK**. The template you selected is added to the right pane with the other certificate templates.
20. Restart the CA (to publish the new template in the Active Directory).

9.2.3 Request Handling

Certification Authorities include settings that define how certificate requests are handled. Intel SCS does not support pending certificate requests. If during configuration the CA puts the certificate into the "Pending Requests" state, Intel SCS returns an error (#35). Thus, you must make sure that the CA and the templates used by Intel SCS are not defined to put certificate requests into a pending state.

For Enterprise and Standalone CAs, request handling is defined in the Request Handling tab (right-click the CA and select **Properties** > **Policy Module** > **Properties**). Make sure that the correct option is selected (highlighted in red in Request Handling tab on the next page).

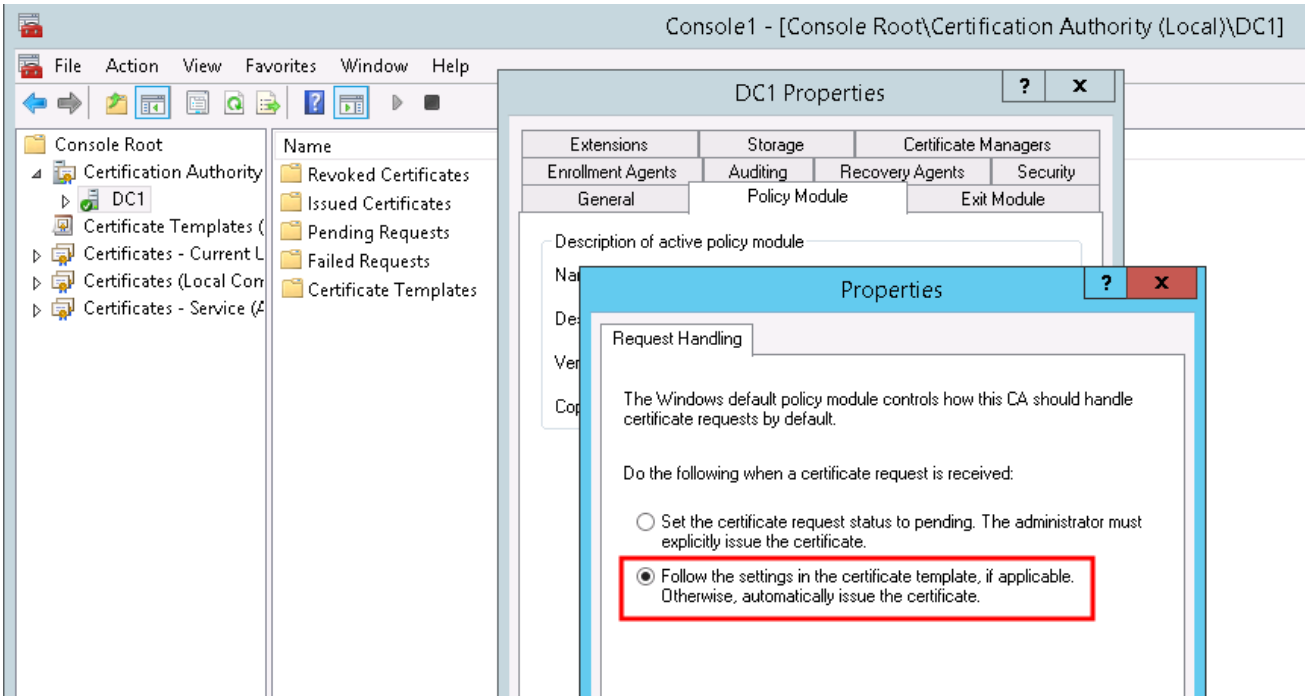


Figure 9-5: Request Handling tab

For Enterprise CAs, you must also make sure that the templates used by Intel SCS are not defined to require approval. Make sure that the **CA certificate manager approval** check box is NOT selected (highlighted in red in Issuance Requirements tab on the next page). To check this setting for a template, right-click it and select **Duplicate Template**, then click the **Issuance Requirements** tab.

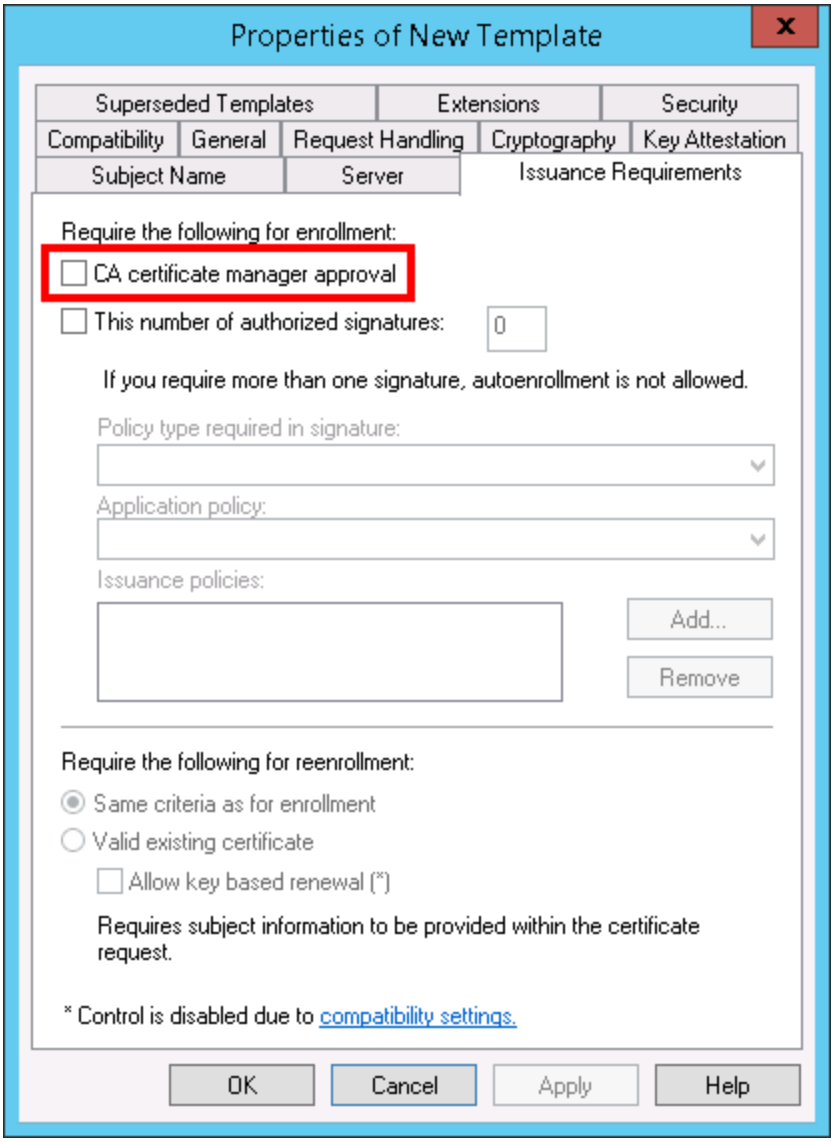


Figure 9-6: Issuance Requirements tab

9.2.4 Running the CA on Windows Server 2003

SCS no longer supports Windows Server 2003. To run CAs on Windows Server 2003, use SCS version 11.1 or earlier.

9.2.5 Required Permissions on the CA

The following access permission on the CA is required for the user account that is running the configuration:

- Request Certificates

To add this permission, do the following:

1. Right-click on the Certification Authority instance in the Console Root tree, and in the resulting Properties dialog box (see Certificate Authority Properties dialog box, Security tab below), click the **Security** tab. You can set the permission here.
2. Click **Apply**.

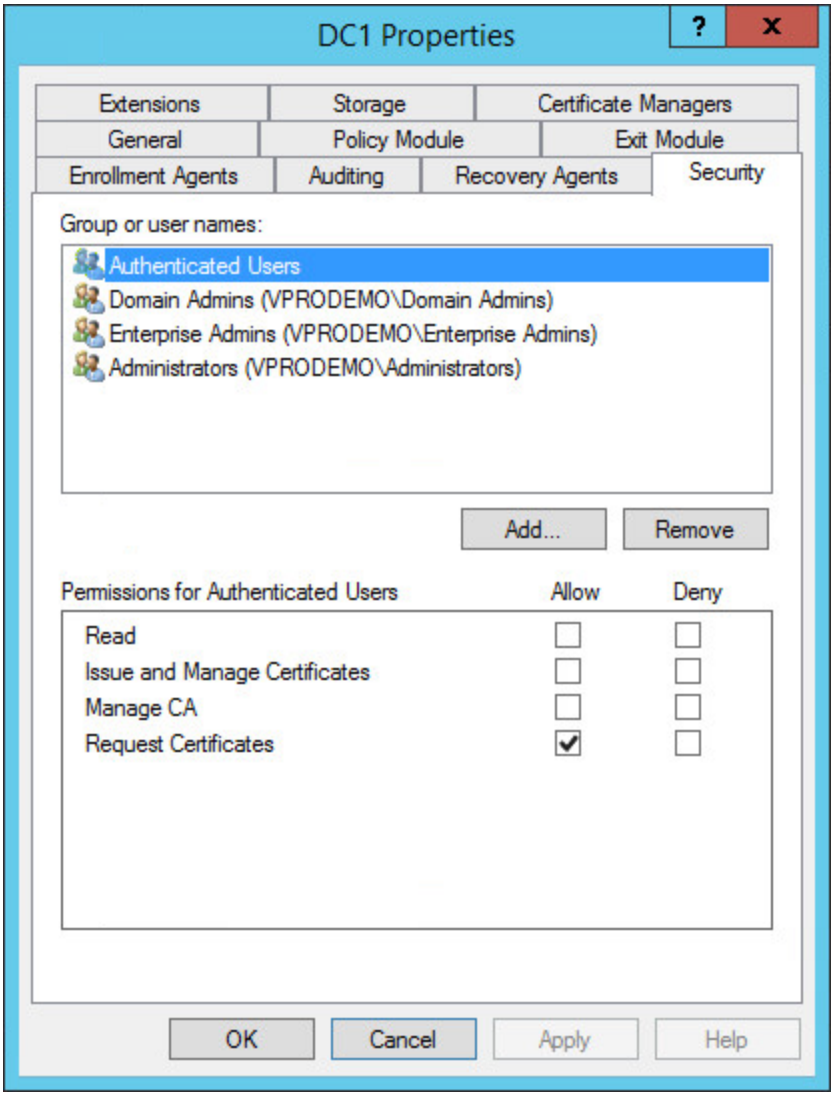


Figure 9-7: Certificate Authority Properties dialog box, Security tab

For an Enterprise root CA, you also need to grant this user account the Read and Enroll permissions on the templates you want to select in the configuration profiles. To do this, do the following:

1. From the Console Root tree, double-click **Certificate Templates**. (See the instructions in Defining Enterprise CA Templates on page 192 if this snap-in is not present.) The list of templates is shown in the right pane.

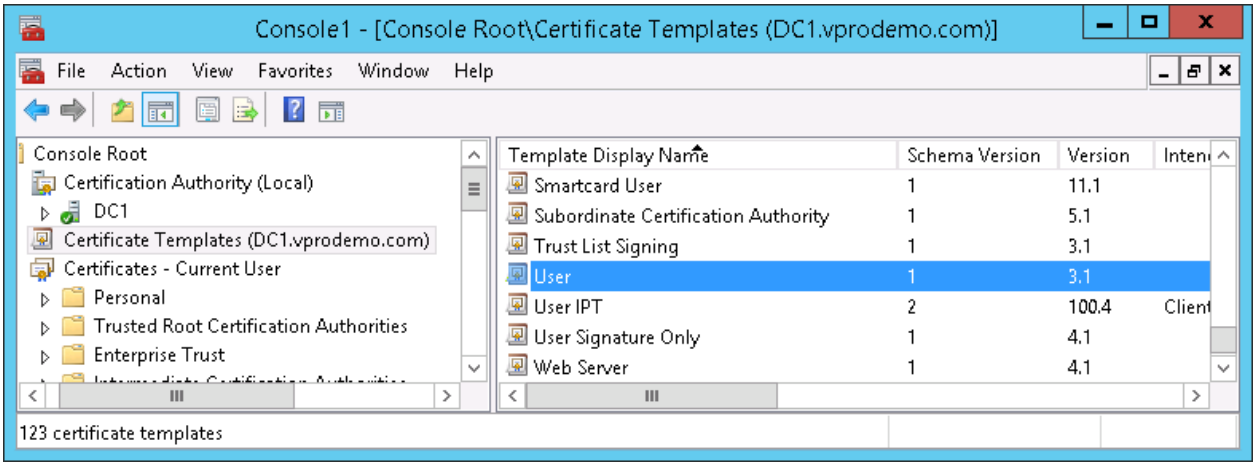


Figure 9-8: Microsoft Management Console

2. In the right-pane, right-click the template to be changed, and select **Properties**. The template's Properties dialog box appears.
3. Click the **Security** tab and make sure the **Allow** boxes are checked for the Read and Enroll permissions, as shown in Template Properties dialog box, Security tab on the next page.

4. Click **Apply**.

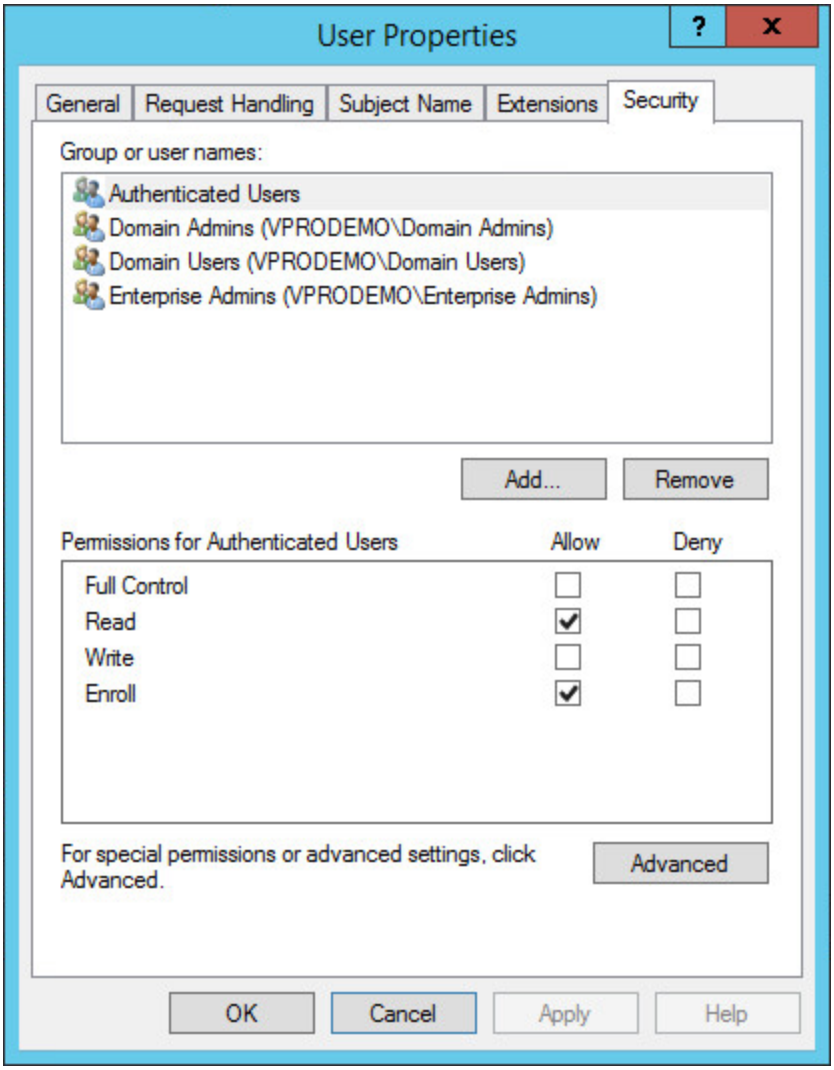
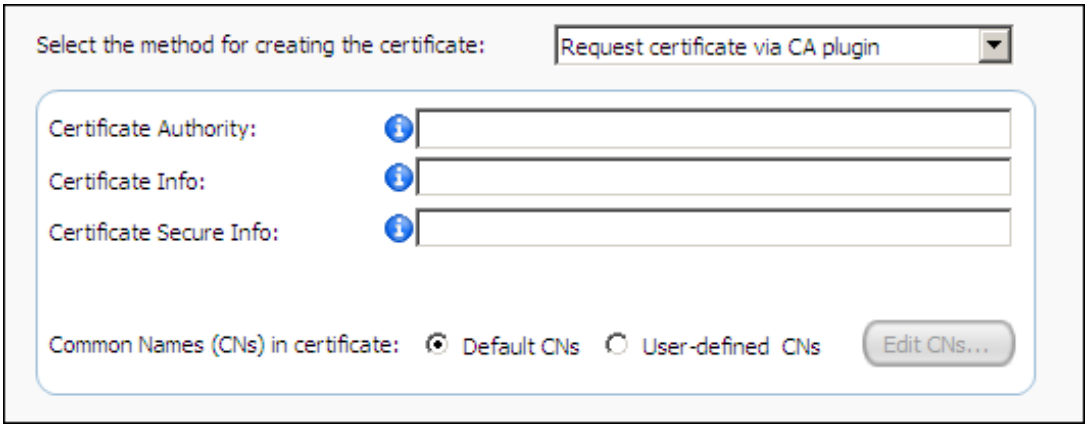


Figure 9-9: Template Properties dialog box, Security tab

9.3 Using Intel SCS with the CA Plugin

By default, Intel SCS requests certificates from a Microsoft CA. Intel SCS can also request certificates from other types of CA by using a "CA plugin". The plugin is installed on the computer running the RCS. Each time that the RCS starts, the plugin is automatically loaded (only one CA plugin can be loaded).

After the plugin is loaded, these fields are shown in each profile window that contains certificate-based authentication options (Remote Access, TLS, 802.1x, EAC):



Note:

- The RCS only loads plugins that are compatible with Intel SCS.
- You can only use the CA plugin option with the `ConfigViaRCSOnly` command sent from the Configurator. No other options are supported.

To setup and use the CA plugin:

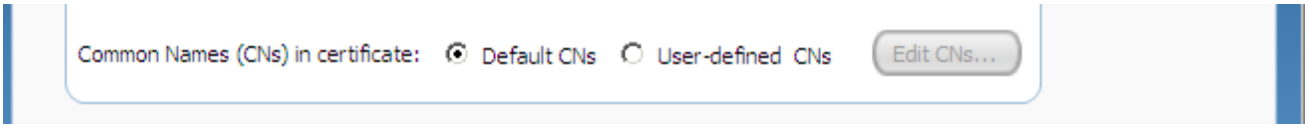
1. On the computer running the RCS, install the CA plugin as described in the installation instructions provided with the plugin.
2. After restarting the RCS, open the console and check that the plugin was successfully loaded (see Certification Authority Plugin on page 80).
3. In the relevant profile window, from the Select the method for creating the certificate drop-down list, select Request certificate via CA Plugin.
4. When the plugin option is selected, these fields are shown:
   - Certificate Authority
   - Certificate Info
   - Certificate Secure Info

   The values that you enter in these fields are not validated by the RCS. If you leave them empty, the default values defined by the plugin will be used. Refer to the plugin documentation for more information.
5. Define the Common Names that will be included in the Subject Name of the generated certificate. For more information, see Defining Common Names in the Certificate on the next page.

9.4 Defining Common Names in the Certificate

The certificate generated by the CA includes Common Names (CNs) in the Subject field and the Subject Alternative Name field.

You can use these options in the profile to define the CNs in the generated certificate:



These fields are shown in each profile window that contains certificate-based authentication options (Remote Access, TLS, 802.1x, EAC).

Default CNs

When you select **Default CNs**, the generated certificate will include these CNs:

- In the Subject field: DNS Host Name (FQDN)
- In the Subject Alternative Name field:
  - DNS Host Name (FQDN)
  - Host Name
  - SAM Account Name (Active Directory account name for the Intel AMT object)
  - User Principal Name
  - UUID of the Intel AMT system

User-defined CNs

This option lets you control which CNs will be included in the generated certificate, and which CN will be put in the Subject Name field.

Note:

Some servers require a specific CN in the Subject Name field:

- The Cisco* Access Control Server (ACS) requires the SAM Account Name
- The Funk* Odyssey* Server requires the Host Name

To define user-defined common names:

1. Select **User-defined CNs**.
2. Click **Edit CNs**. The Advanced Common Name window opens.

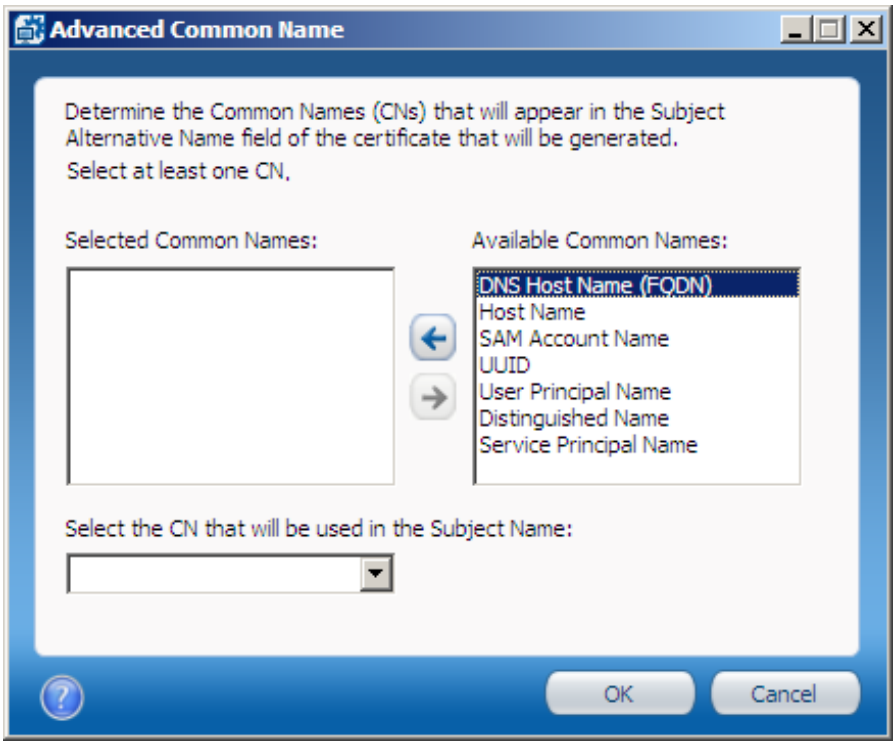


Figure 9-10: Advanced Common Name Window

3. From the Available Common Names list, select the required CNs and click  to add them to the Selected Common Names list. All the selected CNs will be put in the Subject Alternative Name field of the certificate.
4. From the drop-down list, select a CN (from the list of Selected Common Names). This CN will be put in the Subject Name field of the certificate (in addition to the Subject Alternative Name field).
5. Click **OK**. The Advanced Common Name window closes.

9.5 CRL XML Format

If you are using mutual authentication, you can also configure the Intel AMT device with data from a Certificate Revocation List (CRL). Intel SCS does not use the original CRL file supplied by the Certification Authority. The information from the CRL file must be placed in the <CRLs> tag of the configuration profile.

You can use the Configuration Profile Wizard to import the CRL into the configuration profile (see Defining Advanced Mutual Authentication Settings on page 108).

Note:

The profile can contain a maximum of four CRLs. The combined CRLs can contain a maximum total of 64 serial numbers.

This is an example of the XML format required by the Configuration Profile Wizard:

```
<?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://certification.authority.example.1.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="1527822000000000003"/>
</uri>
<uri name="http://certification.authority.example.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>
```

For the serial number attribute:

- 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 printable non-hexadecimal character separator between each pair.

Chapter 10

Setting up Remote Configuration

This chapter describes the prerequisites and procedures to setup remote configuration.

For more information, see:

10.1 About Remote Configuration

This section describes concepts and terms related to the remote configuration option of Intel AMT.

- **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 RCS authenticates to the Intel AMT system, it must do so with a certificate compatible with one of the hashed root certificates. In AMT 11, the default CA hashes have been updated to their SHA256 equivalents for use during PKI provisioning.
- **Self-signed Certificate** – The Intel AMT system produces a self-signed certificate from which the public key can be passed to the RCS.
- **Limited Network Access** – The Configurator 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)** – This (optional) feature can be used to make sure that the RCS will only respond to legitimate remote configuration requests. Before the configuration request is sent to the RCS, an OTP can be set in the Intel AMT device. This OTP can then be sent to the RCS as part of the configuration request. If the RCS is defined to require an OTP, the RCS asks the device to provide the OTP that was set. The RCS compares the OTP sent from the device with the OTP that was sent in the configuration request. If the OTPs are not the same, the RCS will not start the configuration. (The RCS always ignores OTPs sent from systems with Intel AMT 3.x and lower.)

  By default, the RCS is defined to require this OTP validation. You can change this default (see Defining the RCS Settings on page 77). These are the main reasons that you might want to remove this OTP validation:

  - If you want to use WMI commands to send remote configuration requests without an OTP. (For increased security, the Configurator always sends the OTP in the configuration request.)
  - If you want to use jobs to configure unconfigured systems using the RCS (see Configuration via Jobs Fails because of OTP Setting on page 228).
- **Bare Metal Setup and Configuration** – The Intel AMT device can be predefined by the manufacturer to start sending Hello messages as soon as the system is connected to power and to the network. This can occur even if an operating system is not installed on the host system (thus the name "bare metal"). The RCS then configures the system using a script (see Remote Configuration Using Scripts on page 216).

10.2 Prerequisites for Remote Configuration

Before remote configuration can begin, these initial conditions must be met:

- The Intel AMT device must have at least one active hash certificate defined in the Intel MEBX.
- The Intel AMT system must be configured to receive its IP address from a DHCP server. The DHCP server must support option 15 and return the local domain suffix.
- The computer running the RCS must have a certificate with the Server Authentication Certificate OID (1.3.6.1.5.5.7.3.1) and also contain one of these:
  - An OID in the Extended Key Usage field with this value: 2.16.840.1.113741.1.2.3

  - Or -

  - In the Subject Name field, an OU with this value:

    OU=Intel(R) Client Setup Certificate.

    In the Certification Path of this certificate, the thumbprint of the root certificate must be enabled in the Intel AMT hash table.
- The Suffix of the Common Name (CN) in the Subject Name of the RCS certificate must match the domain suffix of the Intel AMT system (see Selecting the Remote Configuration Certificate below).
- For "Bare Metal Setup and Configuration" only: The computer running the RCS must have an alias record with the name "Provisionserver" in the DNS server (or the name defined by the manufacturer in the Intel MEBX). The Intel AMT system must be able to access this DNS server.
- Supported versions of Windows Server include an option to create a custom certificate request using the MMC Certificate snap-in. If you use this option, make sure that this option is NOT selected in the Template drop-down list: **(No Template) CNG Key**. The CNG Key option is selected by default in the Certificate Enrollment wizard but is not supported by Intel SCS. You must change the selected Template to be: **(No Template) Legacy Key**.

10.3 Selecting the Remote Configuration Certificate

Intel AMT validates the RCS remote configuration 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.

For more information and guidelines about how to select this certificate, refer to this document: "An Introduction to Intel AMT Remote Configuration Certificate Selection" available at https://www.intel.com/content/www/us/en/architecture-and-technology/implementation-of-intel-active-management-technology.html.

10.4 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".

These settings are necessary for the certificate to be compatible for remote configuration use:

- The OU or the OID must match the values defined in Selecting the Remote Configuration Certificate on the previous page (the OU is the usual value entered when purchasing a certificate commercially).
- The CN must match the Intel AMT system domain suffix (see Selecting the Remote Configuration Certificate on the previous page).
- 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.

10.4.1 Installing a Vendor Certificate

You can install more than one certificate into the certificate store of the user account running the RCS (`RCSServer.exe`). The RCS selects the certificate suitable for the specific Intel AMT system.

To install a certificate in the RCS users certificate store:

1. On the computer where the RCS is installed, log in as the user running the RCS.
2. Open a command prompt window, enter mmc and press <Enter>. The Microsoft Management Console window opens.
3. If the Certificates plug-in is not installed, perform these steps:
   a. Select **File** > **Add/Remove Snap-in**. The Add/Remove Snap-in window opens.
   b. Click **Add**. The Add Standalone Snap-in window opens.
   c. From the list of available snap-ins, select **Certificates** and click **Add**. The Certificates snap-in window opens.
   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 opens.
5. Click **Next**. The File to Import window opens.
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 opens.

> **Note:**
>
> If the check box named **Enable strong private key protection** can be selected, make sure that it is NOT selected.

Figure 10-1: 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**.

10.4.2 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 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 RCS (`RCSServer.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 opens.
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**.

10.5 Creating and Installing Your Own Certificate

These section describes how you can install your own certificate to enable remote configuration.

10.5.1 Creating a Certificate Template

This procedure describes how to create a remote configuration certificate.

To create the certificate template:

1. From your Certificate Authority server, open the Microsoft Management Console Window.
   a. select **Start** > **Run**. The Run window opens.
   b. Enter mmc and click **OK**. The Microsoft Management Console window opens.
2. If the Certificate Templates plug-in is not installed, perform these steps:
   a. Select **File** > **Add/Remove Snap-in**. The Add/Remove Snap-in window opens.
   b. Click **Add**. The Add Standalone Snap-in window opens.
   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.

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

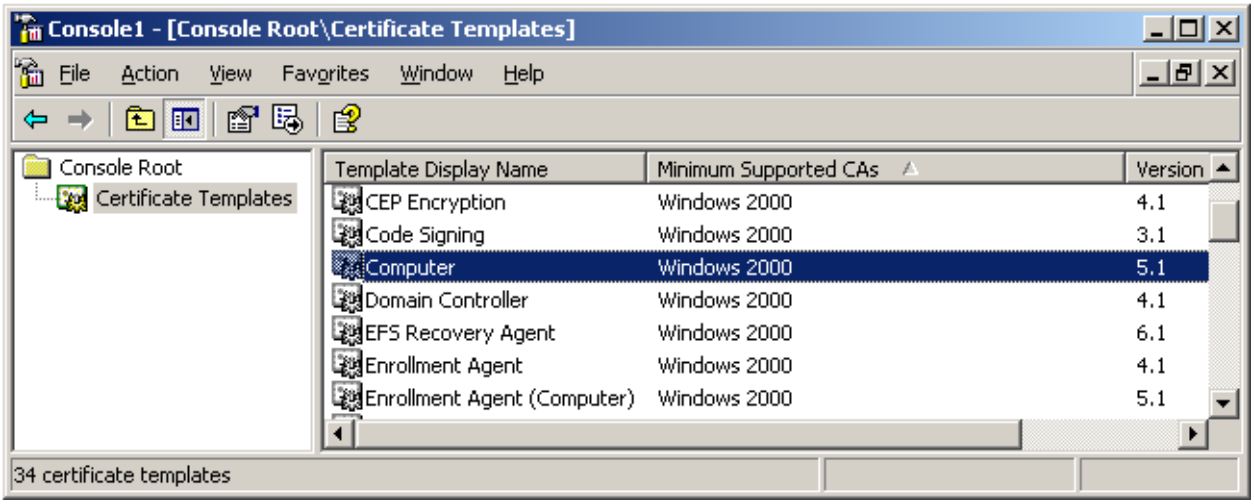


Figure 10-2: Microsoft Management Console

4. In the right-pane, right-click the **Computer** template and select Duplicate Template. The Properties of New Template window opens.

Figure 10-3: Properties of New Template Window

> **Note:**
>
> If the CA is installed on a server running Windows Server 2012 (all x32/64 versions and R2), the Duplicate Template window opens. Make sure that you select Windows Server 2003 Enterprise on the **Compatibility** tab.

5. Click the General tab. Make sure that the **Publish certificate in Active Directory** check box is NOT selected.
6. In the Template display name field, enter a name for the template.
7. Click the **Extensions** tab. From the list of extensions, select **Application Policies** and click **Edit**. The Edit Application Policies Extension window opens.
8. Click **Add**. The Add Application Policy window opens.
9. Click **New**. The New Application Policy window opens.
10. Enter a policy name, and in the Object Identifier field enter this OID for remote configuration: **2.16.840.1.113741.1.2.3**
11. 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.
12. Click the **Subject Name** tab and select **Supply in the request**.
13. Click the **Request Handling** tab and select the **Allow private key to be exported** check box.
14. Click **OK**. The Properties of New Template window closes.

15. Open the **Certification Authority** from Server Manager Tools or type certsrv.msc from Run window. The Certification Authority window opens.
16. From the tree in the left pane, select **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 is now included in the right pane with the other certificate templates.
19. Restart the CA (to publish the new template into Active Directory).

10.5.2 Requesting and Installing the Certificate

This procedure describes how to request and install the certificate on the computer running the RCS (`RCSServer.exe`).

To install the certificate:

1. On the computer running the RCS, open an internet browser and connect to Certificate Services for the Root CA using this naming convention: **http://CA_FQDN/certsrv**. If the CA requires an SSL connection, use this naming convention instead: **https://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 213).
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 RCS) in the Name field.
7. Leave all the other default values and click **Submit**.
8. Install the certificate in the RCS user's certificate store and then restart the RCS.

10.5.3 Entering a Root Certificate Hash Manually in the Intel AMT Firmware

Normally the certificate hashes are programmed in the Intel AMT system firmware by the manufacturer. Alternatively, there is an option to enter the root certificate's hash manually via the Intel MEBX. (The names and locations of menu options might vary slightly in different Intel AMT versions.)

To enter the certificate hash via the Intel MEBX:

1. Open the Root certificate and tab to Details. Keep the Root certificate thumbprint from the thumbprint field for use in step 7.
2. Power on the Intel AMT system and press <Ctrl-P> during boot.
3. When the Intel MEBX menu is displayed, do a full unconfiguration (unprovision).
4. From the Intel 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 Intel MEBX and reboot the Intel AMT system.

10.6 Remote Configuration Using Scripts

Usually, when the RCS configures a system the configuration process is started when the Configurator sends a configuration request to the RCS. In certain conditions, this might not be applicable for your network environment. For example:

- If you want to use the "Bare Metal" option
- If you want to supply the RCS with the configuration data for each system, or start the configuration process from the RCS

Instead of using the Configurator, you can use "Hello" messages and a script.

10.6.1 How the Script Option Works

The RCS requires identification information for each Intel AMT system before it can perform the setup and configuration. The "Hello" message sent from an Intel AMT system contains the UUID of the Intel AMT system.

When a Hello message arrives:

1. The RCS sets environment variables based on values in the Hello message, and activates the script.
2. The script reads the environment variables set by the RCS, and uses them to find the necessary identification information for the Intel AMT system.
3. The script uses the `ConfigAMT` command of the RCS API to send the configuration request to the RCS.
4. The RCS configures the system.

Environment Variables

The RCS sets these environment variables:

- CS_AMT_UUID – The UUID of the system
- CS_AMT_ADDRESS – The IP address of the system
- CS_AMT_CONFIGURATION_METHOD – The configuration mode of the device:
  - 1 – The device has a Private Share Key defined (PID-PPS)
  - 2 – The device is set for PKI authentication
- CS_AMT_PID – The PID of the TLS-PSK key (for PSK only)

Note: TLS-PSK Configuration is not supported on Intel AMT 11 or later.

10.6.2 Preparing to Use Scripts

To use the script option:

- The RCS must be set to listen for Hello messages and to use the script that you supply (see Defining the RCS Settings on page 77).
- The Intel AMT system must be prepared for configuration using one of these methods that use the TLS protocol:
  - Remote Configuration using PKI on page 5
- The Intel AMT system must send a Hello message. This will happen automatically if the system was prepared for "Bare Metal Setup and Configuration" by the manufacturer. If not, you can send a Hello message using the Configurator CLI (see Sending a Hello Message on page 146).

10.6.3 Defining a Script

Script functionality is the responsibility of the IT organization. The script can retrieve the information from an external source or from the host containing the Intel AMT device. For example:

- The script can send a Windows Management Instrumentation (WMI) query to get the FQDN from the host using the IP address sent in the Hello message. This requires the host to be operational and running a version of Microsoft Windows that can process WMI queries.
- The script can get the FQDN from a pre-prepared database or file containing the UUID and FQDN of each Intel AMT device.

Sample Script

Intel SCS includes a sample script (`ConfigAMT.vbs`). You can use the sample script as a basis for reference when creating your script. The script is located in this folder:

`sample_files\hello_listener_sample_files`.

Chapter 11

Troubleshooting

This chapter describes problems you might find when using Intel SCS, and provides their solutions.

For more information, see:

11.1 Damaged RCS Data Files

If one of the data files used by the RCS (in non-database mode) is damaged or missing:

- The Console shows a "login failure" message when trying to connect to the RCS.
- When you try to save a profile, the Console shows an error message.

Solution:

Restore the latest backup version of the data files to the correct location (see Backing up Data on page 54).

If you did not create a backup, do one of these:

- Uninstall and then reinstall the RCS (non-database mode). This creates new empty copies of all the required data files.

- OR-

- In the registry of the computer running the RCS, add a DWORD key with the name "Recover" to this key:
  - 32-bit operating systems: `HKLM\SOFTWARE\Intel\Intel(R) Setup and Configuration Software\12`
  - 64-bit operating systems: `HKLM\SOFTWARE\Wow6432Node\Intel\Intel(R) Setup and Configuration Software\12`

When the RCS starts, it checks if this key exists. If the key exists with a value not equal to zero, the RCS will automatically create a new empty file for each damaged or missing data file. Only damaged or missing data files are replaced.

11.2 Connecting to an RCS behind a Firewall

If you install the RCS on a computer that is protected by a firewall, you might receive error messages when you try to connect to the RCS.

Solution:

You must make sure that the firewall is configured to enable the WMI to connect to the RCS. For more information, refer to the Microsoft Developer Network:

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

11.3 Exit Code 110

This error can occur if both these conditions are true:

1. The certificate chain of the digital certificate cannot be validated locally by the host operating system on the Intel AMT system.
2. The host operating system on the Intel AMT system failed to access the Internet.

Digital certificates contain data about the organization from which they were issued. This data forms a "certificate chain" that ends in a trusted root certificate of a known CA. If the trusted root certificate is not installed in the operating system, Windows uses an automatic update mechanism to download the necessary root certificate from Microsoft.

Some versions of Windows (for example, Windows 8) do not include all the trusted root certificates necessary to validate time-stamped digital signatures. If these systems also do not have Internet access, the automatic update mechanism will fail.

Solutions:

- Make sure that host operating system has access to the Internet. This is the easiest solution because the certificate will be downloaded automatically.
- If you cannot connect the Intel AMT system to the Internet, manually download and install a root certificate update package from the Microsoft update catalog. Select the relevant package for the operating system from this website:

  http://catalog.update.microsoft.com/v7/site/Search.aspx?q=root%20certificate%20update

11.4 Remote Connection to Intel AMT Fails

During configuration, an IP address is set in the Intel AMT device. This IP address is used by management consoles (and Intel SCS) to remotely connect to Intel AMT.

If the IP address is incorrect, these problems might occur:

- Your management console will not be able to connect to the device.
- If you are using the RCS to configure systems:
  - This error: "Post configuration connection to the Intel(R) AMT device failed" in the RCS log file. This error occurs because, after configuration is complete, the RCS tries (and fails) to connect to the device to test the connection.
  - In database mode, the "Connection Status" column in the Console will show that the RCS failed to connect to these systems.

Solutions:

The first step is to check the IP address that is defined in the Intel AMT device. To do this, use the `SystemDiscovery` command. For more information, see Discovering Systems on page 129.

The value of the IP address is located in this tag/registry key:

Configurationinfo > AMTNetworkSettings > AMTWiredNetworkAdapter > IPv4IPSettings > IP.

- If this tag/registry key contains the correct IP address:
  - In the Domain Name System (DNS), make sure that this IP address is associated with the correct FQDN for the Intel AMT system.
  - If you have a Firewall in your network, make sure that the ports used by Intel AMT are not blocked (16992; 16993; 16994; 16995; 5900).
- If this tag/registry key contains a value of "**0.0.0.0**", this means that the device is waiting to be updated by the DHCP server. This can occur after you do any of these:
  - Configure a system to use DHCP, but the system was already configured to use a static IP.
  - Run a "Full" unconfiguration on a system (this sets the system back to the default which uses an IP address from the DHCP server).

  To fix this problem, it is recommended to run this command on the Intel AMT system to immediately update the IP address: ipconfig /renew

After the IP address is correctly defined in the Intel AMT device, all remote connections should work without any problems. In database mode, to change the Connection Status, you can run a job on these systems (for example, a maintenance job). When the job finishes, the RCS will test the connection again and then update the Connection Status.

11.5 Error with XML File or Missing SCSVersion Tag

Errors 37 or 38 are returned by the Configurator if problems exist with the configuration profile XML file. These errors usually occur when the Configurator cannot find the file or read the data that it contains.

Solutions:

- As of Intel SCS 12.2, the encryption algorithm for `SCSEncryption.exe` has been strengthened. If the XML file was encrypted using the discontinued algorithm, decrypt the file using `SCSEncryption.exe`, then re-encrypt it with `SCSEncryption.exe` to encrypt with the new supported algorithm.
- In the command line, make sure that you supplied the correct name for the XML file. For example, if the filename contains spaces, you must supply the filename in quotes (like this: "My Profile").
- Make sure that the profile is a valid profile. Profiles created using Intel SCS 7.0 are NOT supported. These profiles do not have the mandatory `<SCSVersion>` tag. Even if you add the missing `<SCSVersion>` tag, the profile is still invalid because it contains tags and values not supported by the current version of Intel SCS. (Profiles created using Intel SCS 7.1 include this tag and are valid for use by the current Intel SCS.)

  Note:

  Try to open the profile using the Intel AMT Configurator Utility supplied in the current Intel SCS version. To do this, select **Create Settings to Configure Multiple Systems** and browse to the folder containing the profile. If the profile is not shown in the list of profiles it is not a valid profile.

- If the Intel AMT system is running Windows XP, make sure that Service Pack 3 is installed.
- If the profile is encrypted, these errors can occur on Intel AMT systems running Windows 7. This is because of a known Microsoft issue. Install this hotfix: http://support.microsoft.com/kb/981118.

11.6 Reconfiguration of Dedicated IP and FQDN Settings

Reconfiguration can fail when all these conditions are true:

1. The Intel AMT device was configured with an FQDN and IP different from the host operating system (for example, by using a dedicated network settings file).
2. The dedicated network settings file contains FQDN and IP values different from those currently defined in the Intel AMT device.
3. Intel SCS needs to reconfigure the device using the new values in the dedicated network settings file.

Solution:

Make sure you supply the current IP address or FQDN of the Intel AMT device in the <CurrentAMTAddress> tag of the dedicated network settings file.

11.7 Disjointed Namespaces

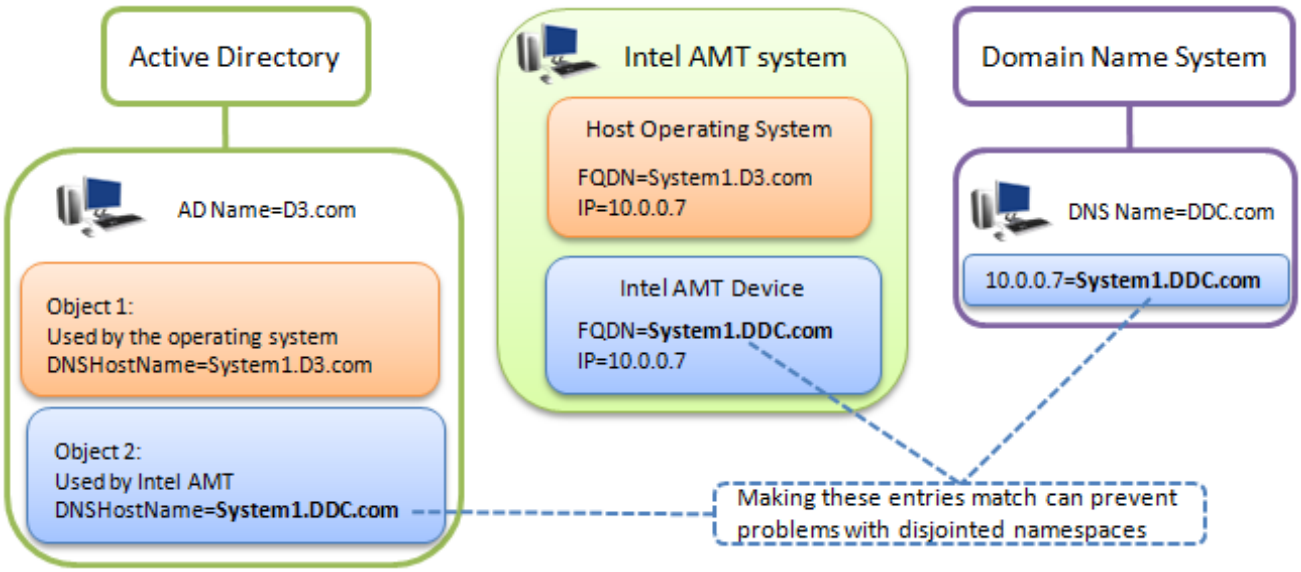
A disjointed namespace occurs when the primary Domain Name System (DNS) suffix of a computer does not match the DNS domain of which it is a member. Defining a network environment with disjointed namespaces (intentionally or accidentally) can cause many different types of communication and authentication failures.

For Intel AMT, these failures can be related to:

- Configuration/Reconfiguration
- Authentication using Kerberos users in the Access Control List (ACL)
- Authentication using Transport Layer Security (TLS)

Solution:

If integration with Active Directory (AD) is enabled, during configuration Intel SCS sends a request to create an AD object for the Intel AMT device. Some of the entries in this object define parameters used in Kerberos tickets. For example, the DNS Host Name and the Service Principal Names (SPNs). If these entries in the AD object are configured using the correct DNS name, problems with disjointed namespaces can be avoided. For example, "Object 2" in this diagram was created by Intel SCS using an FQDN in the Intel AMT device (System1.DDC.com) that matches the DNS name.



To implement this solution:

1. Check in the DNS to find the correct name that can be resolved using DNS resolution. This name needs to be inserted into the FQDN of the Intel AMT device.
2. Use Intel SCS to configure/reconfigure the Intel AMT device with the required FQDN. Intel SCS includes several options for the source it can use when inserting the FQDN into the Intel AMT device (see Defining IP and FQDN Settings on page 123).

11.8 Disjointed Hostnames and AD Objects

A disjointed hostname occurs when the hostname in the Domain Name System (DNS) is not the same as the hostname assigned in Windows. This can occur when the hostname in DNS contains characters that are not valid characters in a Windows hostname. Disjointed hostnames usually occur when the network environment is using a DNS hierarchy and needs to support different DNS zones. To support this hierarchy, the hostname in DNS can be defined by joining the DNS zones and using periods as a separator. Because periods are not valid in the Windows hostname, the FQDN in Windows must be defined differently. For example by using underscores instead of periods, as shown in this table (where the hostname part of the FQDN is marked in yellow):

Example	Record in DNS	FQDN in Host Operating System
#1	10.0.0.7=System1.DNS1.DDC.com	System1_DNS1.DDC.com
#2	10.0.0.8=System1.DNS2.DDC.com	System1_DNS2.DDC.com

If integration with Active Directory (AD) is enabled, during configuration Intel SCS sends a request to create an AD object for the Intel AMT device. By default, the object is created using the hostname part of the FQDN that Intel SCS configured in the Intel AMT device. The value of the FQDN that Intel SCS configures in the Intel AMT device is defined in the configuration profile. Most of these options take the hostname from the operating system.

The `DNS Look Up FQDN` option takes the name returned by an "nslookup" on the IP address of the on-board wired LAN interface. In the examples above, this would mean that the FQDN defined in the Intel AMT device is the same as the FQDN shown in the Record in DNS Column. When multiple records in DNS have identical values for the first part of the hostname (in this example "System1"), this can cause problems when creating AD objects. This is because the AD object is created using only the first part of the hostname, up to the first period. The result is that only one AD object will be created even though multiple Intel AMT devices exist.

Solution:

In the AD Integration window, select the **Always use the OS Host Name for the new AD Object** check box (see Defining Active Directory Integration on page 92).

When this check box is selected, the AD object will always be created using the hostname defined in the operating system.

Note:

This option is not supported when using jobs with a job operation type of "Configuration".

11.9 Kerberos Authentication Failure

If integration with Active Directory (AD) is enabled, during configuration Intel SCS creates an AD object for the Intel AMT device. The values of the Service Principal Name (SPN) attribute in this object are used in Kerberos tickets during AD authentication.

If the AD forest contains more than one object representing the same Intel AMT device, the Kerberos authentication will fail. This is because identical SPN values exist for different objects. The AD does not know which SPN to use, and thus an error occurs.

Multiple objects can be created during reconfiguration when you change the AD Organizational Unit (ADOU) defined in the profile (see Defining Active Directory Integration on page 92). If you do not use the `/ADOU` flag in the CLI, Intel SCS does not know the location of the old object and thus cannot delete it.

Solution:

Make sure that the AD forest contains only one AD object for each Intel AMT device.

If not:

1. Manually delete the object from the old ADOU.
2. Wait approximately 15 minutes, or manually purge the Kerberos tickets. (You can use the `Klist.exe` application to purge the tickets.)

11.10 Error: "Kerberos User is not Permitted to Configure"

Usually, this error will occur if all these conditions are true:

- The requested operation will change the FQDN setting in the Intel AMT device, or the Intel AMT Active Directory object.
- The requested operation is run using a Kerberos admin user.
- The password of the default Digest admin user is not defined in the profile or supplied in the CLI command (using the `/AdminPassword` parameter).

This is to prevent losing connection to the device when changing these settings.

Solution:

Define the Digest admin password in the profile or the CLI command.

11.11 Error: "The Caller is Unauthorized."

Intel AMT includes a security mechanism to prevent brute force attacks that are trying to "crack" the Digest admin password. If a brute force attack is detected, connection to the device is blocked and error messages like these are recorded in the log file:

Intel(R) AMT connection error 0xc000521d: The caller is unauthorized.

After connection to the device is blocked, this error will continue to occur even when trying to connect with the correct password.

Solution:

Wait for approximately one hour and then try the requested operation again.

11.12 Error when Removing AD Integration (Error in SetKerberos)

For some Intel AMT 4.x and 5.x systems, this warning can occur during reconfiguration with a profile that contains TLS settings but disables Active Directory (AD) integration:

```
error in SetKerberos (1) Failed while calling WS-Management call
SetKerberosSettings
```

This warning occurs only if the system was initially configured with a profile containing TLS settings and AD integration enabled. The result is that configuration is completed (including TLS), but the AD integration is not disabled.

Solution:

This is a known limitation that was solved in versions 4.2.30 and 5.2.30 of the Intel AMT firmware. For systems with this problem:

1. Reconfigure the system using a profile that disables TLS and Active Directory.
2. Reconfigure the system using a profile that enables and defines the required TLS settings.

11.13 Failed Certificate Requests via Microsoft CA

Due to Microsoft limitations, creation of the certificate might fail in these situations

- If the FQDN of the Intel AMT device is longer than 64 characters
- If the certificate Subject Name is longer than 256 characters
- If the CN in the Subject Name field is the Distinguished Name, and this Distinguished Name is longer than 256 characters

Solution:

Make sure that the values in the generated certificate will not exceed the maximum values listed above. A possible solution for large values in the Subject Name field is to define a CN that will contain less characters (see User-defined CNs on page 205).

11.14 Delta Profile Fails to Configure WiFi Settings

In certain conditions, reconfiguring a configured system using a "Delta" profile containing WiFi Connection settings does not enable WiFi in the Intel AMT device. The configuration will complete with warnings, and the log file will include this error:

A WSMAN command returned an error: GetField: no such field named "LinkPolicy"

This can occur if all these conditions are true:

- The system was configured using a profile that disabled WiFi in the Intel AMT device (the profile did not include WiFi Connection settings).
- The system was then reconfigured using a Delta profile that included WiFi Connection settings, but did NOT include Power Management settings.
- The Delta profile was created in a version of Intel SCS earlier than Intel SCS 8.1.

Solution:

A check box was added to the Network Configuration window of the profile (Enable WiFi connection also in S1-S5 operating power system states). This solves the problem because the power management settings for the wireless NIC can now be configured using a delta profile. During upgrade/migration, this check box is not added to delta profiles (to support backwards compatibility).

To add the check box and reconfigure the system:

1. Open the delta profile in Intel SCS (When you open the profile, the check box is added.)
2. In the Network Configuration window, verify that the status of the new check box is what you require (selected/not selected).
3. Save the profile.
4. Reconfigure the system using the Delta profile.

11.15 Disabling the Wireless Interface

Intel AMT includes a wireless interface that can be enabled or disabled during configuration. You can define this setting in the profile using the WiFi Connection check box (see Defining Profile Optional Settings on page 91).

To disable the interface after it has been enabled, you can remove the WiFi Connection settings from the profile and then reconfigure the system. But, reconfiguration does not always disable the wireless interface. This is a known limitation of some versions of the Intel AMT Firmware.

Solution:

If reconfiguration did not close the wireless interface:

1. Unconfigure the system.
2. Reconfigure the system using a profile containing the settings that you want.

11.16 Configuration via Jobs Fails because of OTP Setting

A configuration operation, defined in a job, will fail on a system when all of these conditions are true:

1. The system is in the "Unconfigured" status.
2. The system is defined to use PKI authentication during configuration.
3. The RCS is defined to require a One-Time Password (OTP) when a system is configured using PKI authentication. This setting is defined in the Configuration Options tab (see Defining the RCS Settings on page 77).

The failure occurs because the RCS cannot remotely set the OTP in the Intel AMT device. (This is usually done by the Configurator when it sends the configuration request to the RCS.)

Solution:

Remove the requirement for an OTP. To do this, select **None** in the Advanced Configuration Options section of the Configuration Options tab.

Note:

Changing this setting to None will also cancel the OTP requirement for all future remote configuration requests sent from the Configurator. For more information about OTP, see About Remote Configuration on page 209.

11.17 Configuration Fails with Exit Code 111

Management Engine (ME) firmware versions 6.x, 7.x, 8.x, 9.x, 10.x, 11.0, 11.5, and 11.6 are considered vulnerable for Intel-SA-00075. It is highly recommended that you upgrade your ME firmware. Read the Public Security Advisory at https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00075.html for more information.

11.18 Configuration Fails with SSL Error

This error can occur during remote configuration of an Intel AMT system with an unsupported version of SSL/TLS encryption.

Note:

TLS 1.0 has been deprecated as the security protocol for Intel SCS communication with Intel AMT. The TLS 1.0 protocol has identified security vulnerabilities, including CVE-2011-3389 and CVE-2014-3566. Intel SCS will default to TLS 1.1 or TLS 1.2 (depending on your Intel AMT version) to encrypt communication between Intel SCS software components and Intel AMT.
Users can enable TLS 1.0 protocol support for backwards compatibility during installation/upgrade of the Remote Configuration Server (RCS). For instructions on how to enable or disable TLS 1.0 protocol support, see Configuring Transport Layer Security (TLS) Protocol Support on page 72.