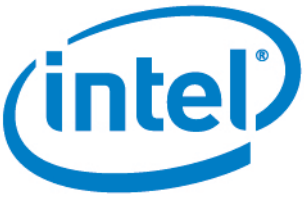


# Intel® AMT Configuration Utility

## User Guide

Version 10.0

Document Release Date: December 18, 2014

## 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.

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 may require enabled hardware, specific software, or services activation. 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.

© 2014 Intel Corporation

# Table of Contents


**Chapter 1 Introduction ..... 1**

1.1 What is the Intel AMT Configuration Utility? ..... 2

1.2 Quick Start Guide ..... 2

1.3 What is Intel AMT? ..... 3

1.4 Configuration Methods and Intel AMT Versions ..... 3

1.4.1 Host-based Configuration ..... 4

1.4.2 SMB/Manual Configuration ..... 4

1.5 Intel AMT and Security Considerations ..... 5

1.5.1 Password Format ..... 5

1.5.2 File Encryption ..... 5

1.5.3 Digital Signing of Files ..... 6

1.5.4 Recommendations for Secure Deployment ..... 7

1.5.5 Control Modes ..... 7

1.5.6 User Consent ..... 8

1.5.7 Security After Configuration ..... 9

1.5.8 Access to the Intel MEBX ..... 9

1.6 Admin Permissions in the Intel AMT Device ..... 10

1.6.1 Default Admin User (Digest) ..... 10

1.6.2 User-Defined Admin User (Kerberos) ..... 10

1.7 Maintenance Policies for Intel AMT ..... 12

1.7.1 About Maintenance Tasks ..... 12

1.7.2 Manual/Automatic Maintenance using the CLI ..... 14

1.8 Support for KVM Redirection ..... 16

1.9 Support for Integration with Intel SBA ..... 17

**Chapter 2 Prerequisites ..... 18**

2.1 Getting Started Checklist ..... 19

2.2 Supported Intel AMT Versions ..... 23

2.3 Supported Operating Systems ..... 24

2.4 Support for a Workgroup Environment ..... 25

2.5 Required User Permissions ..... 26

**Chapter 3 Using the Configuration Utility ..... 27**

3.1 Starting the Configuration Utility ..... 28

3.2 Configuring/Unconfiguring Individual Systems ..... 29

3.3 Configuring a System ..... 30

3.3.1 Defining IP and FQDN for a Single System ..... 31

3.3.2 Encrypting the Profile ..... 34

3.4 SMB/Manual Configuration ..... 35

3.5 Unconfiguring a System ..... 38

3.6 Using the Profile Designer ..... 39
3.7 Defining Manual Configuration (Multiple Systems) ..... 40

**Chapter 4 Defining Intel AMT Profiles ..... 42**
4.1 About Intel AMT Profiles ..... 43
4.2 Creating a Configuration Profile for Intel AMT ..... 44
4.2.1 Saving the Configuration Profile ..... 45
4.3 Defining the Profile Scope ..... 47
4.4 Defining Profile Optional Settings ..... 48
4.5 Defining Active Directory Integration ..... 49
4.5.1 Defining Additional Security Groups ..... 50
4.5.2 Defining Additional Object Attributes ..... 51
4.6 Defining the Access Control List (ACL) ..... 52
4.6.1 Adding a User to the ACL ..... 53
4.6.2 Using Access Monitor ..... 55
4.7 Defining Home Domains ..... 56
4.8 Defining Remote Access ..... 57
4.8.1 Defining Management Presence Servers ..... 58
4.8.2 Defining Remote Access Policies ..... 60
4.9 Defining Trusted Root Certificates ..... 61
4.10 Defining Transport Layer Security (TLS) ..... 63
4.10.1 Defining Advanced Mutual Authentication Settings ..... 64
4.11 Defining Network Setups ..... 66
4.11.1 Creating WiFi Setups ..... 68
4.11.2 Creating 802.1x Setups ..... 70
4.11.3 Defining End-Point Access Control ..... 73
4.12 Defining System Settings ..... 75
4.12.1 Defining IP and FQDN Settings ..... 78

**Chapter 5 Using the Configurator ..... 81**
5.1 About the Configurator ..... 82
5.2 CLI Syntax ..... 82
5.3 Configurator Log Files ..... 83
5.4 CLI Global Options ..... 83
5.5 Verifying the Status of Intel AMT ..... 84
5.6 Discovering Systems ..... 84
5.7 Configuring Systems ..... 86
5.8 Configuring a System using a USB Key ..... 87
5.8.1 Power Package GUIDs ..... 89
5.9 Maintaining Configured Systems ..... 90
5.10 Unconfiguring Intel AMT Systems ..... 92
5.11 Running Scripts with the Configurator ..... 95

5.11.1 Scripts Run by the Configurator ... 96
5.11.2 What if a Failure Occurs? ... 97
5.11.3 Script Runtime and Timeout ... 98
5.11.4 Parameters Sent in Base64 Format ... 98
5.12 Configurator Return Codes ... 99

**Chapter 6 Preparing the Certification Authority ... 104**
6.1 About Certification Authorities ... 105
6.2 Using Intel SCS with a Microsoft CA ... 105
6.2.1 Standalone or Enterprise CA ... 105
6.2.2 Required Permissions on the CA ... 105
6.2.3 Request Handling ... 106
6.2.4 Defining Enterprise CA Templates ... 107
6.3 Using Predefined Files Instead of a CA Request ... 113
6.4 Defining Common Names in the Certificate ... 114
6.5 CRL XML Format ... 116

**Chapter 7 Troubleshooting ... 117**
7.1 Configuration Utility Error: "Cannot Configure Intel AMT" ... 118
7.2 The Configuration Utility Takes a Long Time to Start ... 118
7.3 Problems Using Configuration Utility on a Network Drive ... 119
7.4 Exit Code 88 ... 120
7.5 Exit Code 110 ... 120
7.6 Remote Connection to Intel AMT Fails ... 121
7.7 Error with XML File or Missing SCSVersion Tag ... 122
7.8 Reconfiguration of Dedicated IP and FQDN Settings ... 122
7.9 Disjointed Namespaces ... 123
7.10 Kerberos Authentication Failure ... 124
7.11 Error: "Kerberos User is not Permitted to Configure.." ... 124
7.12 Error: "The Caller is Unauthorized." ... 124
7.13 Error when Removing AD Integration (Error in SetKerberos) ... 125
7.14 Failed Certificate Requests via Microsoft CA ... 125
7.15 Delta Profile Fails to Configure WiFi Settings ... 126
7.16 Disabling the Wireless Interface ... 126

# Chapter 1

## Introduction

This guide describes how to use the Intel® AMT Configuration Utility, referred to in this guide as the "Configuration Utility".

> **Note:**
>
> The Configuration Utility is a component of Intel® Setup and Configuration Software (Intel® SCS) that you can use to configure Intel® Active Management Technology (Intel® AMT). This guide only includes information about options available when the Configuration Utility is used on its own, or with the Configurator. For information about the other components and features of Intel SCS refer to the `Intel(R)_SCS_User_Guide.pdf`.

This chapter describes the Configuration Utility and other important background information.

For more information, see:


1.1 What is the Intel AMT Configuration Utility? ..... 2
1.2 Quick Start Guide ..... 2
1.3 What is Intel AMT? ..... 3
1.4 Configuration Methods and Intel AMT Versions ..... 3
1.5 Intel AMT and Security Considerations ..... 5
1.6 Admin Permissions in the Intel AMT Device ..... 10
1.7 Maintenance Policies for Intel AMT ..... 12
1.8 Support for KVM Redirection ..... 16
1.9 Support for Integration with Intel SBA ..... 17

# 1.1 What is the Intel AMT Configuration Utility?

The Intel AMT Configuration Utility (Configuration Utility) is a wizard that you can use to configure Intel AMT.

You can use the Configuration Utility in two different ways:

- Run the Configuration Utility on an Intel AMT system to configure Intel AMT
- Create XML profiles that can be used to configure Intel AMT on multiple systems. You can then supply these profiles in the Command Line Interface (CLI) commands of the Configurator. The Configurator will configure Intel AMT with the settings in the profile.

# 1.2 Quick Start Guide

This is a quick start guide to help you decide how to use the Configuration Utility to configure Intel AMT systems.

How you use the Configuration Utility depends on these four conditions:

### #1 The Number of Systems to Configure

The Configuration Utility is the easiest deployment method and is recommended when a small number of systems need to be configured. To use this method, see:

- Starting the Configuration Utility on page 28
- Configuring/Unconfiguring Individual Systems on page 29

When a large number of systems need to be configured, use the Profile Designer to create an XML profile and then use the Configurator to do the configuration. For more information, see:

- Using the Profile Designer on page 39
- Configuring Systems on page 86

### #2 The Intel AMT Versions in the Network

The versions of Intel AMT in your network will define which configuration methods you can use (see Configuration Methods and Intel AMT Versions on the next page).

### #3 The Security Requirements

The Intel AMT device gives access to the computer even when the operating system is not running. This means that a virus/person could use the Intel AMT device to bypass the security measures defined in the operating system and take over the computer. For more information about security, see Intel AMT and Security Considerations on page 5.

### #4 The Requirements of Your Network

You can configure several optional Intel AMT features using the configuration profiles. But, before you create a the profile, refer to the Getting Started Checklist on page 19.

**Note:**

The SMB/Manual Configuration method does not use configuration profiles.

# 1.3 What is Intel AMT?

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 |
|---|---|---|
| 1 | Host-based Configuration | 6.2 and higher |
| 2 | SMB/Manual Configuration | 4.0 and higher |
| 3 | One-Touch Configuration using PSK | 2.1 and higher |
| 4 | Remote Configuration using PKI | 2.2, 2.6, 3.0 and higher |
| Configuration methods #3 and #4 are not supported by the Configuration Utility. These configuration methods use the Remote configuration Service (RCS) component of Intel SCS. For more information about Intel SCS, refer to the `Intel(R)_SCS_User_Guide.pdf`. | | |

## 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 42).

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 7).

You can use the Configuration Utility to quickly define a profile and then immediately configure the system (see Configuring a System on page 30).

Alternatively, you can use the Profile Designer to create an XML profile and then use the Configurator to do the configuration. For more information, see:

- Using the Profile Designer on page 39
- Configuring Systems on page 86

## 1.4.2 SMB/Manual Configuration

The SMB/Manual configuration method lets you configure the Intel AMT device with basic configuration settings. Configuration is done locally at the Intel AMT system with a USB key containing a configuration file (`Setup.bin`).

After configuration, the Intel AMT device is put in one of these modes:

- **Small Medium Business (SMB) Mode** – Intel AMT 4.x and 5.x devices are put in this mode. Advanced (optional) Intel AMT features are not available to devices in this mode.
- **Manual Mode** – Intel AMT 6.x and higher devices are put in this mode. All Intel AMT features are available to devices in this mode if a third-party application can configure them.

You can use the Configuration Utility to create the `Setup.bin` file. For more information, see:

- SMB/Manual Configuration on page 35
- Defining Manual Configuration (Multiple Systems) on page 40

Alternatively, you can use the `ConfigViaUSB` command of the Configurator (see Configuring a System using a USB Key on page 87).

**Note:**

This method is not available for systems with Intel AMT 2.x and 3.x because they cannot read the `Setup.bin` file.

# 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 16).
- 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

The Configuration Utility uses XML files for the host-based configuration method. These files can contain passwords and other information about your network. To protect this data, each profile created or edited by the Configuration Utility is encrypted (with a password that you supply).

The XML profiles are encrypted using this format:

- Encryption algorithm: AES128 using SHA-256 on the provided password to create the key
- Encryption mode: CBC
- Initialize Vector (IV) is the first 16 bytes of the Hash

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 P@ssw0rd
  ```

- To decrypt an XML file named NetworkSettings.xml:

  ```
  SCSEncryption.exe Decrypt c:\NetworkSettings.xml P@ssw0rd
  ```

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

**Note:**

When encrypting additional XML files, you must use the same password that was used to encrypt the exported profile.

## 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 83). 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 120.
- 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 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 5).
- 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 the previous page).
- 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.

## 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 9).
- **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
  - IDE-Redirection (IDE-R)
  - KVM Redirection
  - To remotely set BIOS boot options
  - To change the source for remote boot (for example, boot from PXE)

## 1.5.7 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.

Transport Layer Security (TLS) is a protocol that secures and authenticates communications across a public network. The Public Key Infrastructure (PKI) 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.

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.

**Note:**

TLS-PKI is not available for Intel AMT devices in SMB mode.

## 1.5.8 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 or using a USB key, 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, or when creating the USB key.

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**.

**Note:**

For information about the RCS and the Unified Configuration process, refer to the `Intel(R)_SCS_User_Guide.pdf`.

# 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 password(s) of the Intel AMT "admin" accounts configured in your systems, it will not be possible to manage or reconfigure Intel AMT on those systems. 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 75).

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. 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) below.

## 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 52).
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 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.
  - You must NOT add the credentials of a domain user to the profile (see Saving the Configuration Profile on page 45).

# 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.

## 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 SMB/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 10.

## 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 49).
2. Use the `ConfigAMT` command of the Configurator CLI (see Configuring Systems on page 86).

**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 using the CLI

Maintenance tasks are done using the `MaintainAMT` command of the Configurator CLI (see Maintaining Configured Systems on page 90).

For more information about the Configurator, see Using the Configurator on page 81.

The `MaintainAMT` command includes 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.

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

Table 1-2: 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.) |

| Key/Value | Description |
|---|---|
| `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.) |
| `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.)<br>**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 52). 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 75.
  - 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.

# 1.9 Support for Integration with Intel SBA

Intel® Small Business Advantage (Intel® SBA) provides an out-of-the-box hardware-based security and productivity suite designed for the small business user. Intel SBA is pre-installed by the computer manufacturer or supplier, but is only configured when the end user wants to start using its features. Some Intel SBA features can configure and define settings in the Intel ME (just like Intel AMT).

For more information about Intel SBA, see http://www.intel.com/go/sba/index.htm.

Some Intel® vPro™ platforms can support both Intel SBA and Intel AMT.

When Intel vPro platforms are configured by Intel SBA, the functionality of Intel AMT is not activated. Intel AMT is activated by configuring the computer using Intel SCS.

On these supported platforms, you have two choices:

- **Uninstall Intel SBA** – Prevent your users access to Intel SBA functionality. To do this, you must uninstall Intel SBA.
- **Integrate with Intel SBA** – Allow your users to continue using Intel SBA functionality after Intel AMT is configured.

### Important Information About Integration:

- To detect if Intel SBA is installed, you can use the `SystemDiscovery` CLI command of the Configurator (see Discovering Systems on page 84). Data about Intel SBA is located in the `SBAServiceInfo` section of the discovery data output.
- The "integration" option is supported only by the host-based configuration methods available in Intel SCS (`ConfigAMT` and `MaintainAMT`). If Intel SBA is installed, these methods will automatically try to integrate with Intel SBA.
- During integration, Intel SCS "takes control" of the Intel ME from Intel SBA. To do this, Intel SCS creates a special Digest user account for Intel SBA. This user account is only given the limited permissions that Intel SBA requires. Intel SBA will then automatically use this user account when it needs to define a setting in the Intel ME.
- Some Intel SBA functionality can only operate correctly if the power management setting is configured to Always on (S0-S5). This is also the recommended setting for Intel AMT (see Power Management Settings on page 76). If the configuration profile is defined with a power management setting of Host is on (S0), this is what will occur:
  - If Intel SBA is already configured, the power management setting will NOT be changed and will remain configured to Always on (S0-S5). This is to prevent "breaking" Intel SBA. A warning message is recorded in the log file that the power management setting was not changed.
  - If Intel SBA is installed but not configured, the power management setting will be configured to Host is on (S0). Intel SBA will be put in the "Incompatible" integration mode and will not be allowed to change this setting. Later, if Intel SBA is configured, Intel SBA features that require the capability to wake up the platform will not be available.

# Chapter 2

## Prerequisites

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

For more information, see:


2.1 Getting Started Checklist ..... 19

2.2 Supported Intel AMT Versions ..... 23

2.3 Supported Operating Systems ..... 24

2.4 Support for a Workgroup Environment ..... 25

2.5 Required User Permissions ..... 26

# 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?**<br>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.<br>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.<br>By default, this is how Intel SCS configures the FQDN (hostname.suffix):<br>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.<br>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 78. | ❑ |
| 2 | IP | **How does your network assign Internet Protocol (IP) addresses?**<br>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.<br>By default, Intel SCS configures the Intel AMT device to get the IP address from a DHCP server.<br>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 78. | ❑ |
| 3 | Domains | **Do you want to limit access to Intel AMT based on domain location?**<br>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 56).<br>**Note:**<br>• 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.<br>• 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?**<br>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.<br>**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)?**<br>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.<br>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.<br>Before you can integrate Intel AMT with your AD, you must:<br>• 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.<br>• Give Create/Delete permissions in the OU you created to the user account running the Intel SCS component doing the configuration<br>After the OU is created, you must define it in the configuration profile (see Defining Active Directory Integration on page 49). | ❑ |

| Getting Started Checklist for Intel SCS | | | |
|---|---|---|---|
| 6 | CA | **Does your network use a Certification Authority (CA)?**<br>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:<br>• Which type of CA do you have?<br>• If you have a Microsoft CA, which type (Standalone or Enterprise)?<br>• On which operating system is the CA installed?<br>• What is the name and location of the CA in the network? (Will the same CA be used for all Intel AMT features?)<br>• What Common Name (CN) to put in the certificate created for each feature?<br>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.<br>• 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.<br>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 107. | ❑ |
| 7 | TLS | **Does your management console require the Intel AMT system to use Transport Layer Security (TLS)?**<br>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.<br>TLS is defined in the Transport Layer Security window of the configuration profile (see Defining Transport Layer Security (TLS) on page 63).<br>**Note:** 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. | ❑ |

| Getting Started Checklist for Intel SCS | | | |
|---|---|---|---|
| 8 | 802.1x | **Does your network use the 802.1x protocol?**<br>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:<br>• Which 802.1x protocol is used in your network?<br>• 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).<br>802.1x is defined in the Network Configuration window of the configuration profile (see Creating 802.1x Setups on page 70).<br>**Note:** These are prerequisites for 802.1x:<br>• Integration with Active Directory (item #5 in this checklist)<br>• A Certification Authority (item #6 in this checklist). If using Microsoft CA, the CA must be an Enterprise CA.<br>• 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. | ❑ |
| 9 | EAC | **Does your network use End-point Access Control (EAC)?**<br>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:<br>• 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.<br>• 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.<br>EAC is defined in the Network Configuration window of the configuration profile (see Defining End-Point Access Control on page 73).<br>**Note:** These are prerequisites for EAC:<br>• Integration with Active Directory (item #5 in this checklist)<br>• A Certification Authority (item #6 in this checklist). If using Microsoft CA, the CA must be an Enterprise CA.<br>• 802.1x (item #8 in this checklist) | ❑ |

| Getting Started Checklist for Intel SCS | | | |
|---|---|---|---|
| 10 | Remote Access | **Does your network have a Management Presence Server (MPS)?**<br>The remote access feature lets Intel AMT systems (versions 4.x and higher) 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. If you need to define Remote Access, this is the data that you need to collect:<br>• What is the location (FQDN or IP address) and listening port of the MPS?<br>• Do you want to use certificate-based authentication or password-based authentication?<br>Remote Access is defined in the Remote Access window of the configuration profile (see Defining Remote Access on page 57).<br>**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 and the LMS are usually installed by the manufacturer. If they are missing, or you need to reinstall them, contact the manufacturer of your system to get the correct versions for your system.

**Note:**

Support for versions of Intel AMT lower than version 6.2 is deprecated. You can still use Intel SCS 10.0 to configure Intel AMT 6.1 and lower. But, Intel SCS 10.0 was not validated on these versions and thus the results cannot be guaranteed. Support agreements for Intel SCS 10.0 do not include support for issues related to versions of Intel AMT lower than version 6.2. The information in this guide related to these versions is provided for informational purposes only.

# 2.3 Supported Operating Systems

You can use the Configuration Utility on these operating systems:

- Windows* 8.1 Pro
- Windows 8.1 Enterprise
- Windows 8 Pro
- Windows 8 Enterprise
- Windows 7 Professional (SP1)
- Windows 7 Enterprise (SP1)
- Windows XP Professional (SP3)

## Additional Requirements

- The Configuration Utility requires version 3.5 of Microsoft .NET Framework (SP1) to be installed on the computer.
- 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.
- 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 Configuration Utility. The 800 x 600 screen resolution is not supported.

# 2.4 Support for a Workgroup Environment

You can configure and use most Intel AMT settings on systems in a peer-to-peer network (a Workgroup). This table shows settings that require services that are not usually available in a Workgroup.

Table 2-1: Intel AMT Settings

<table>
<tr><th>#</th><th>To define this setting...</th><th>You must have...</th></tr>
<tr><td>1</td><td>Active Directory Integration</td><td rowspan="4">Access to an Active Directory (AD)<br>Note:<br>• You must configure setting #1 if you want to configure settings #2, #3, or #4<br>• Settings #3 and #4 also need access to a CA</td></tr>
<tr><td>2</td><td>Kerberos Users</td></tr>
<tr><td>3</td><td>802.1x Setups</td></tr>
<tr><td>4</td><td>Endpoint Access Control (EAC)</td></tr>
<tr><td>5</td><td>Transport Layer Security (TLS)</td><td rowspan="2">Access to a Certification Authority (CA)<br>Note: If you define Remote Access to use password-based authentication, access to a CA is not necessary.</td></tr>
<tr><td>6</td><td>Remote Access</td></tr>
<tr><td colspan="3">In a Workgroup without access to a Domain you cannot configure settings #1 - #4 on Intel AMT systems. You can configure settings #5 and #6, but only on systems with Intel AMT 6.2 and higher.</td></tr>
</table>

Users in a Workgroup do not have the necessary permissions to connect to the AD or the CA. This means that the Intel SCS component, which is running on a computer in the Workgroup, cannot access the AD/CA.

Thus, to configure these settings in a Workgroup, you must use one of these methods:

## Method #1: Supply a user with the necessary permissions

1. In the Profile Designer, create a profile with the settings that you want to configure.
2. When you save the profile, in the "Finish" window, supply the username and password of a user that has permissions to connect to the AD/CA.

## Method #2: Prepare the necessary data in files

1. In the Profile Designer, create a profile with the settings that you want to configure.
2. To define Active Directory Integration, select the "Path to file containing ADOU information" option (see Defining Active Directory Integration on page 49).
3. For each setting with which you want to use certificate-based authentication, select the "Use certificate from a file" option (see Using Predefined Files Instead of a CA Request on page 113).

# 2.5 Required User Permissions

The permissions required by the user account running the Configuration Utility (or the Configurator) depend on the state of the Intel AMT device.

## Unconfigured Systems

The local user account running the Configuration Utility must have administrator permissions in the operating system. On operating systems with User Account Control (UAC), the Configuration Utility must be "Run as administrator". If the Configuration Utility 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. If the user account does not have the required permissions, you must add the credentials of a domain user with these privileges to the profile (see Saving the Configuration Profile on page 45).

## 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 Configuration Utility 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 Configuration Utility with a local user account with administrator permissions on the Intel AMT system. On operating systems with (UAC), the Configuration Utility must be "Run as administrator".

# Chapter 3

## Using the Configuration Utility

This chapter describes how to use the Configuration Utility.

For more information, see:


3.1 Starting the Configuration Utility ..... 28
3.2 Configuring/Unconfiguring Individual Systems ..... 29
3.3 Configuring a System ..... 30
3.4 SMB/Manual Configuration ..... 35
3.5 Unconfiguring a System ..... 38
3.6 Using the Profile Designer ..... 39
3.7 Defining Manual Configuration (Multiple Systems) ..... 40

# 3.1 Starting the Configuration Utility

The Configuration Utility does not require installation. You can run the Configuration Utility from a local drive, a mapped network drive, or a USB key.

> **Note:**
>
> Each window of the Configuration Utility includes context sensitive help that shows when you press F1.

To start the Configuration Utility, open the `ACU_Wizard` folder and double-click **ACUWizard.exe**. The Welcome window opens.

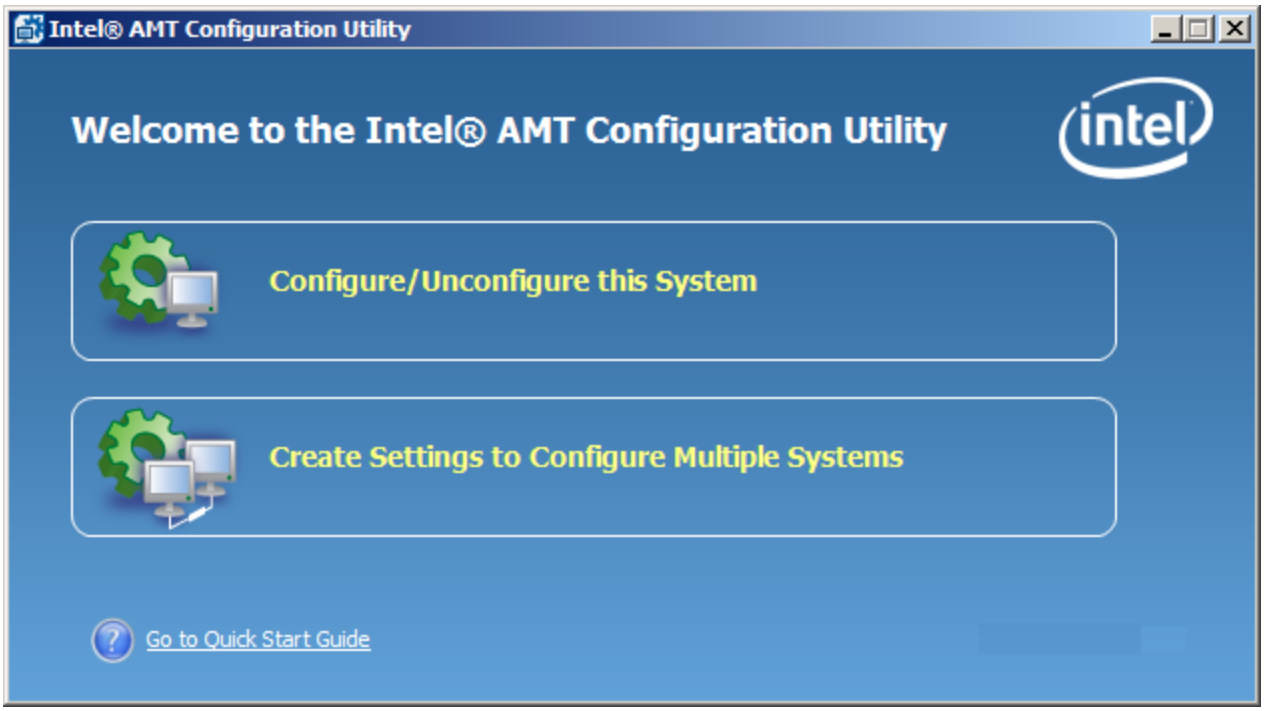



Figure 3-1: Welcome Window

The Welcome window includes these options:

- **Configure/Unconfigure this System**

  This option lets you directly configure Intel AMT systems. You can only select this option if the computer is an Intel AMT system. For more information, see Configuring/Unconfiguring Individual Systems on the next page.

- **Create Settings to Configure Multiple Systems**

  This option, available when you run the Configuration Utility from any location, lets you:

  - Create configuration profiles – See Using the Profile Designer on page 39
  - Create a USB key for manual configuration – See Defining Manual Configuration (Multiple Systems) on page 40

# 3.2 Configuring/Unconfiguring Individual Systems

The Configuration Options window lets you define Intel AMT settings on individual Intel AMT systems.

### To configure/unconfigure Intel AMT:

1. From the Welcome window, click **Configure/Unconfigure this System**. The Configuration Options window opens.

Figure 3-2: Configuration Options Window

2. Select the task and click **Next**:
   - **Configure via Windows** – Use the host-based configuration method or the unified configuration process to configure this system (see Configuring a System on the next page).
   - **Configure via a USB Key** – Use the SMB/Manual method to configure this system (see SMB/Manual Configuration on page 35).
   - **Unconfigure** – Unconfigures the system (see Unconfiguring a System on page 38).

# 3.3 Configuring a System

The Configure via Windows window lets you configure systems with Intel AMT 6.2 and higher. Configured systems are reconfigured.

Configuration is done locally (host-based configuration) using the settings in a configuration profile. The configuration profile is an XML file named `Profile.xml`, and is located in the same folder as the Configuration Utility. If `Profile.xml` does not exist, it is created with default settings. Optionally, you can edit the settings in the profile before starting the configuration. If you make changes, they are saved in `Profile.xml` and will be available for the next systems you configure. You can use the same profile for all systems in your network, or edit the settings for each system.

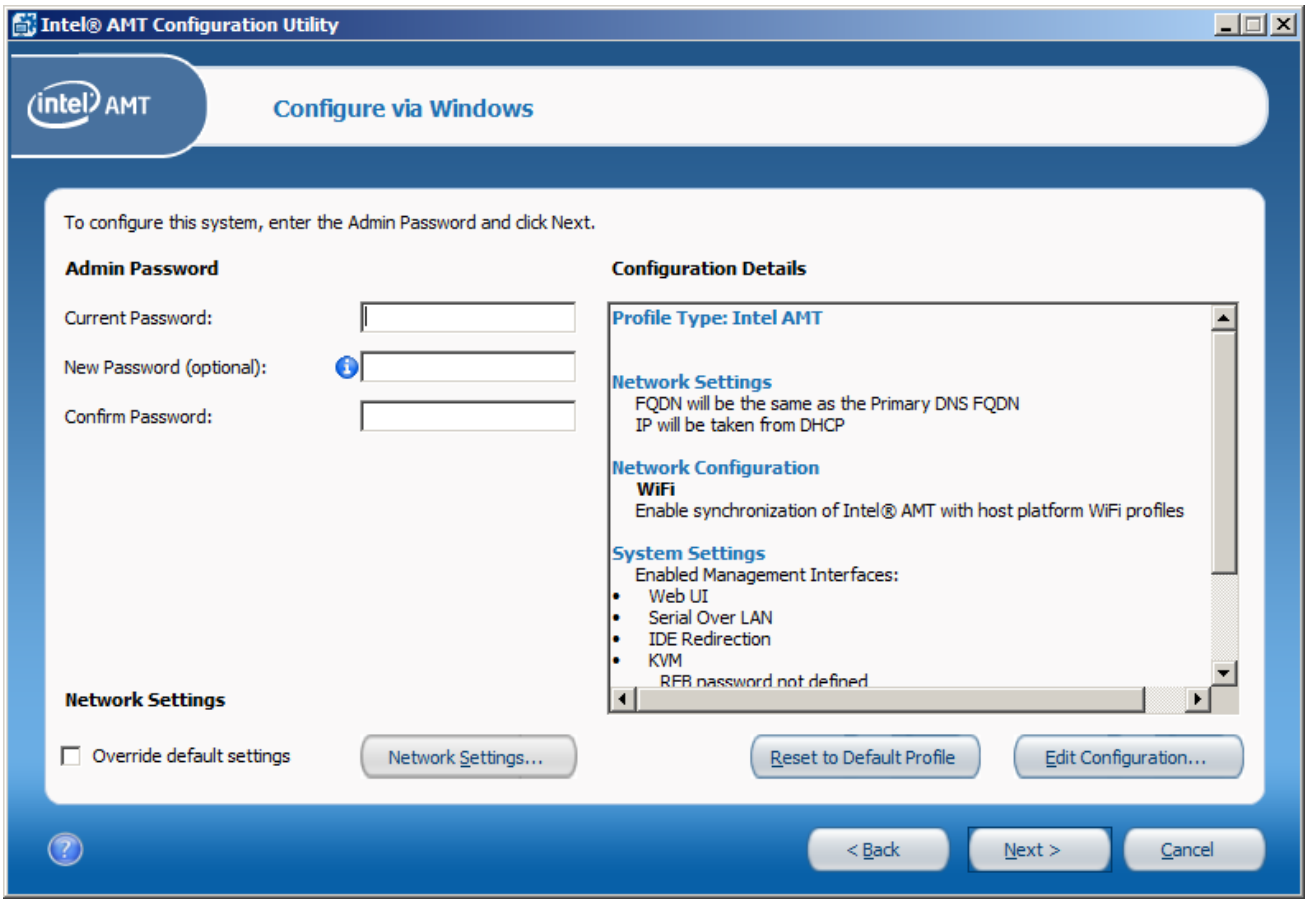



Figure 3-3: Configure via Windows

### To configure an Intel AMT system:

1. From the Configuration Options window, select **Configure via Windows**. The Configure via Windows window opens.

2. In the Admin Password section, enter the password for the default Administrator user in the Intel AMT device:
   - **Current Password** – This field is enabled only if the system is configured. The password that you supply here is used to gain access to the Intel AMT device. If the user account running the Configuration Utility is defined in the device as an administrator, you do not need to supply this password.
   - **New Password/Confirm Password** – If the system is unconfigured, you must define a password in these fields. The Configuration Utility sets this password in the Intel AMT device during configuration, and then saves it in the `Profile.xml` file. Each time that you run the Configuration Utility, the password from the Profile.xml file is automatically put in these fields. You can use the same password for all systems, or change the password for each system that you configure. If you want to change the password of a configured system, enter the new password in these fields.

     For information about the required format, see Password Format on page 5.
3. (Optional) If necessary, you can change the default network settings that the Configuration Utility will put in the Intel AMT device. To do this, select **Override default Settings** and click **Network Settings** (see Defining IP and FQDN for a Single System below).

   **Note:**

   The default network settings that the Configuration Utility puts in the device will operate correctly for most network environments.
4. (Optional) You can change the default settings in `Profile.xml` before you start configuration. To do this, click **Edit Configuration** (see Creating a Configuration Profile for Intel AMT on page 44).

   **Note:**

   If you want to cancel all changes that were made to the profile and revert to the default profile, click **Restore to Default Profile**.
5. If the profile is not encrypted, click **Next** and define an encryption password in the Profile Encryption window (see Encrypting the Profile on page 34).
6. If the profile is already encrypted, click **Configure**. The system is configured with Intel AMT and can be accessed by management consoles.

## 3.3.1 Defining IP and FQDN for a Single System

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. The Configuration Utility puts these settings in the Intel AMT device.

### To change the default IP and FQDN settings:

1. From the Configure via Windows window, click **Network Settings**. The Network Settings window opens.

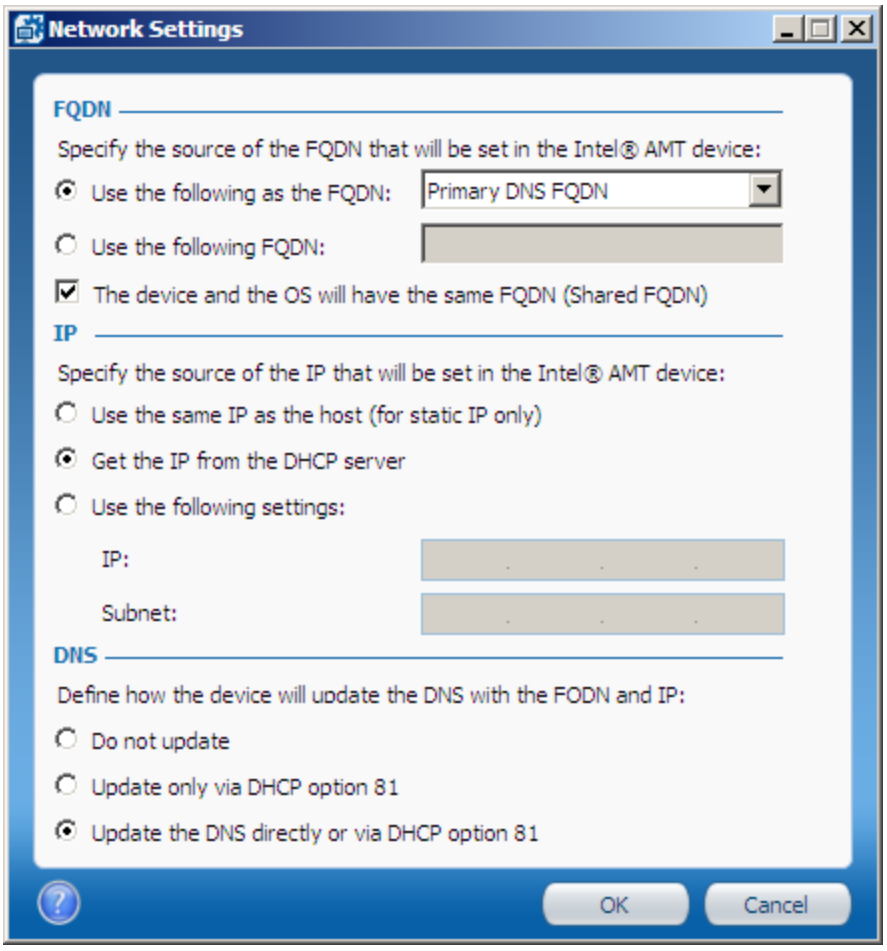



Figure 3-4: Network Settings Window

2. 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 card.
     - **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 card.
   - **Use the following FQDN** – Enter the FQDN you want to set in the device.

3. (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 this setting is 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)**.
4. From the IP section, select the source for the IP settings:
   - **Use the same IP as the host (for static IP only)**
   - **Get the IP from the DHCP server**
   - **Use the following settings** – Enter the IP and subnet address
5. 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.)
6. Click **OK**. The Network Settings window closes and the Profile.xml is updated with the changes that you made.

## 3.3.2 Encrypting the Profile

The `Profile.xml` file, used by the Configuration Utility, contains passwords and other data about your network environment. To protect this data, each profile created or edited by the Configuration Utility is encrypted (with a password that you supply).

When configuring a system, if the profile is not encrypted yet, you must define a password in the Profile Encryption window.

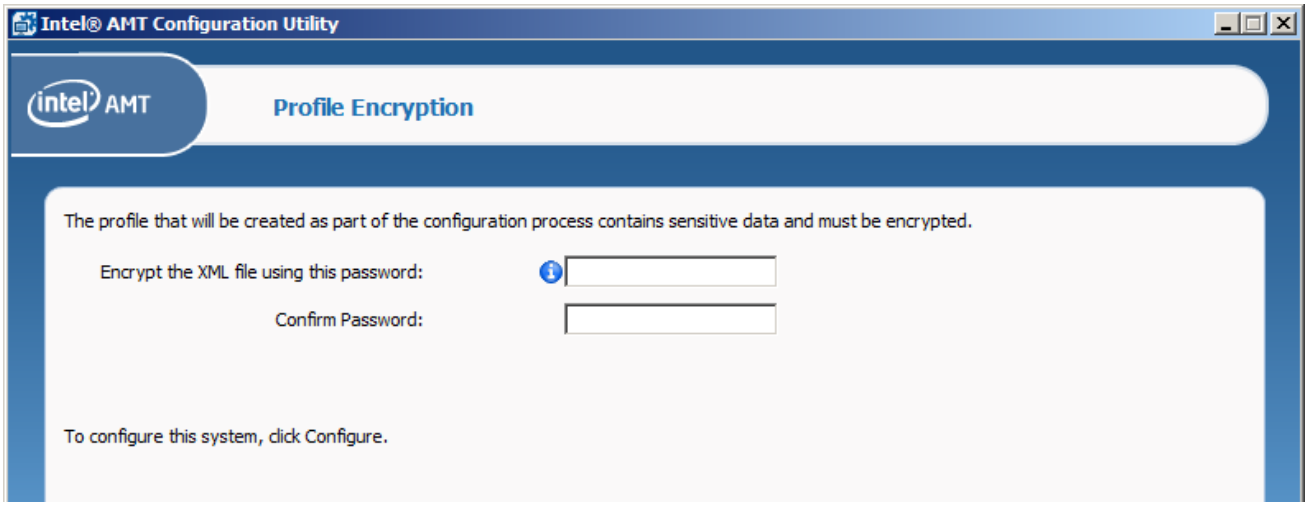



Figure 3-5: Profile Encryption Window

### To encrypt the profile:

1. In the password fields, enter a password that will be used to encrypt the profile. For information about the required format, see Password Format on page 5.
2. Click **Configure**. The profile is encrypted using the password you entered. The system is then configured with Intel AMT and can be accessed by management consoles.

After the profile is encrypted, this window will show each time that you use the Configure via Windows option of the Configuration Utility.

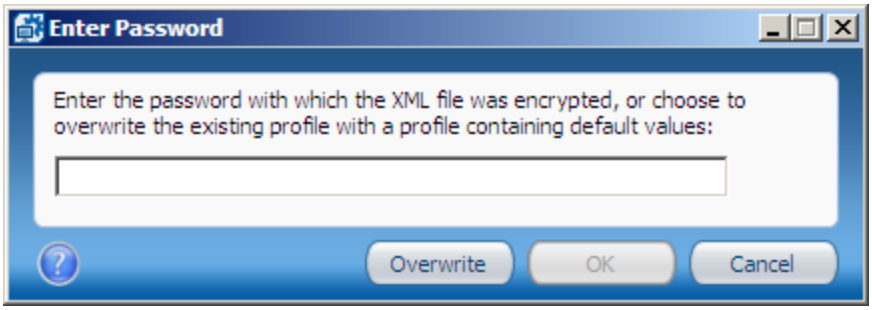



Figure 3-6: Enter Password Window

To use the encrypted profile, you must enter the password used during encryption and then click **OK**. Alternatively, you can click **Overwrite**. If you do this, the Profile.xml file is deleted and replaced with a new `Profile.xml` file that contains default settings.

# 3.4 SMB/Manual Configuration

This procedure describes how to configure an Intel AMT system using a USB key.

> **Note:**
>
> This option is available only for systems with Intel AMT 4.0 and higher. For more information, see SMB/Manual Configuration on page 4.

### To configure an Intel AMT system:

1. From the Configuration Options window, select **Configure via USB Key**. The Configure via USB Key window opens.

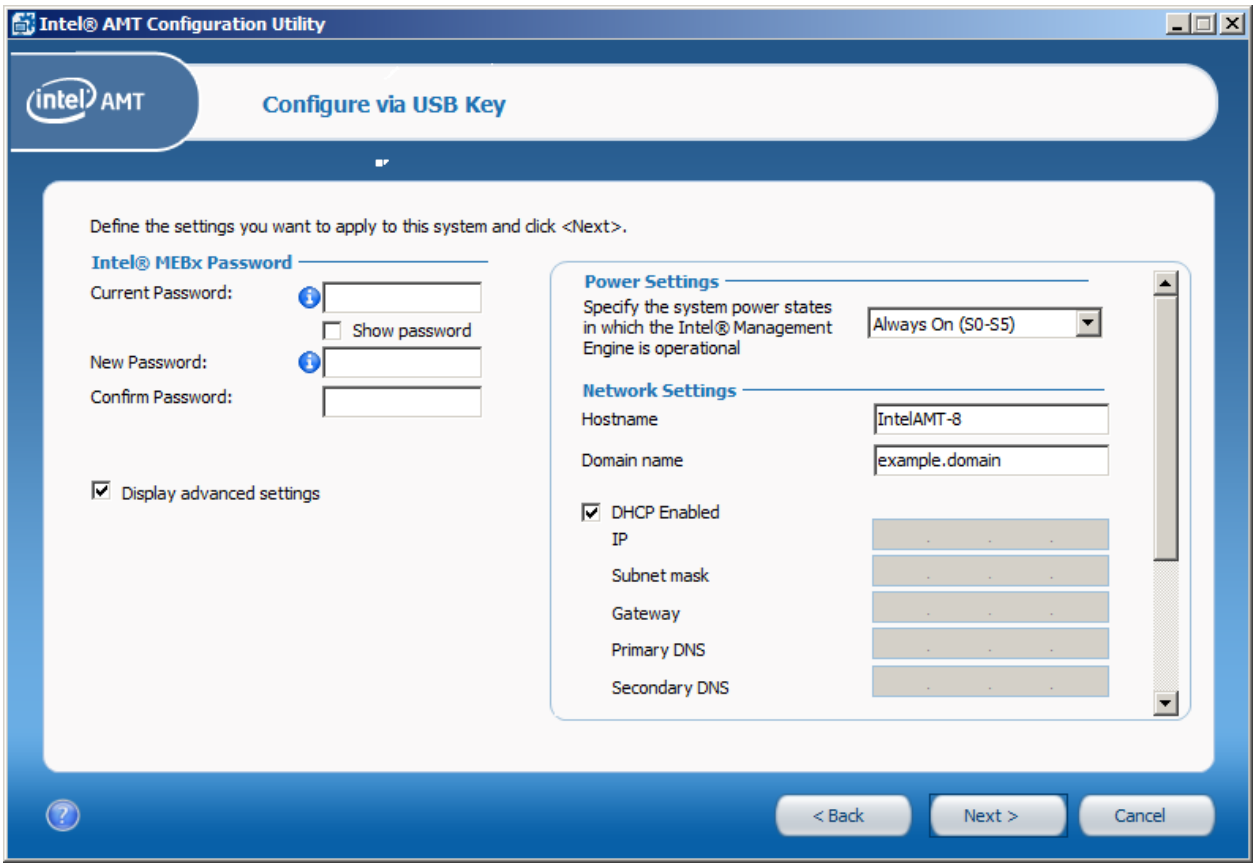



Figure 3-7: Configure via USB Key Window

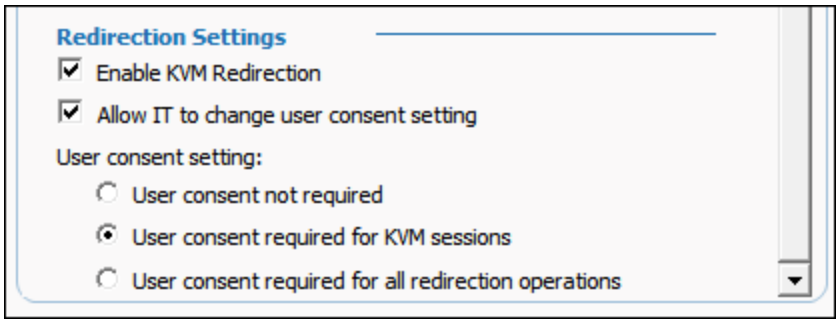
2. In the MEBx Password section, enter the password for the Intel MEBX:
   - **Current Password** – The Configuration Utility always puts the default password of unconfigured systems ("admin") in this field. If this is not the password in the Intel MEBX, enter the correct password. If you do not supply the correct password, configuration will fail.
   - **New Password** – The new password to put in the Intel MEBX. For the first configuration it is mandatory to change the Intel MEBX password. For reconfiguration you must also enter a value here, but it can be the same as the Current Password.

     For information about the required format, see Password Format on page 5.

     **Note:**

     The passwords are not encrypted on the USB key. Make sure that you restrict access to the USB key.

3. (Optional) Select **Display advanced settings** to view or edit the default settings that the Configuration Utility will define for this system:
   - **Power Settings** – Defines in which power states (of the host system) the Intel AMT device will operate.
     - **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.
   - **Network Settings** – By default, the Configuration Utility configures the Intel AMT device with the hostname and the domain name defined in the operating system. This is the recommended setting, but you can change these settings if necessary for your network environment. By default, the Configuration Utility also uses the Dynamic Host Configuration Protocol (DHCP) server to configure the IP address of the device. If you are not using DHCP in your network, clear the **DHCP Enabled** check box and enter the network IP addresses.
   - **Redirection Settings** – These settings are shown only for systems with Intel AMT 6.0 and higher:

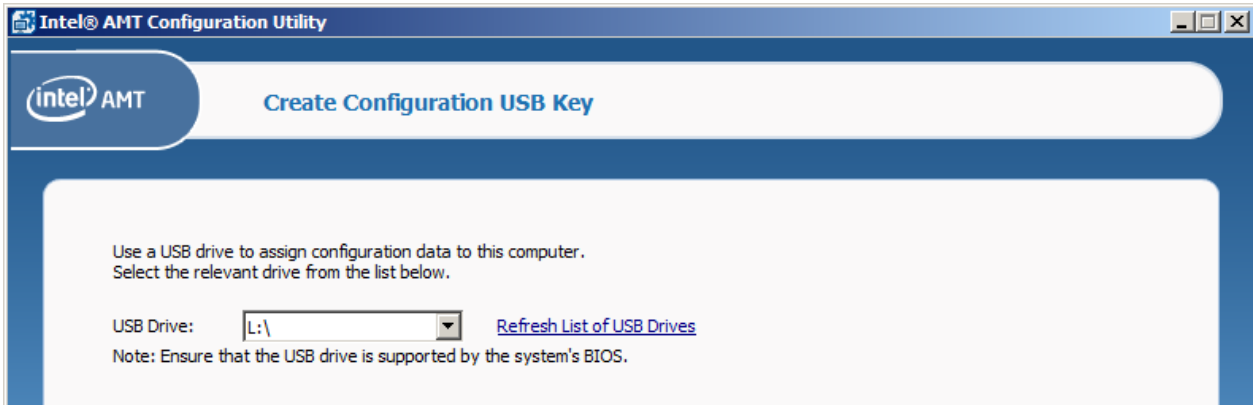
     
     

     Select the settings:
     - **Enable KVM Redirection** – Enables support for KVM redirection
     - **Allow IT to change user consent setting** – Enables changes to the user consent setting in the Intel AMT device to be done remotely
     - **User consent setting** – Defines for which redirection operations user consent is mandatory. For more information, see User Consent on page 8.

4. Put a USB key in the Intel AMT system (this USB key will be formatted in step 7).

> **Note:**
>
> The Configuration Utility does not restrict the size of USB key you can use. But, the computer BIOS must fully support the selected USB key and be able to do a reboot from it.

5. Click **Next**. The Create Configuration USB Key window opens.




6. From the USB Drive drop-down list, select the drive letter of the USB key (you cannot select a USB key if you are using it to run the Configuration Utility).
7. Click **Next**. A message is shown warning that the USB key will be formatted.
8. Click **Yes**. The Configuration Utility creates a configuration file (Setup.bin) on the USB key. When complete, the USB Key Ready window opens with information about the success or failure of the process.
9. Click **Finish**. The Configuration Utility closes.
10. Make sure that only the USB key that you selected in step 6 is connected to the system and reboot the system. During the reboot, a message is shown on the screen:

```
Found USB Key for provisioning
Continue with Auto Provisioning (Y/N)
```

11. Type "Y" and press <Enter>. The settings are put in the device and a new message is shown on the screen:

```
Configuration settings for the USB file were successfully applied
Press any key to continue with system boot...
```

12. Remove the USB key from the system and press a key to continue the reboot. The system is now configured with Intel AMT and can be accessed by management consoles.

> **Note:**
>
> After configuration, the data in the Setup.bin file on the USB key is deleted (but the file is not deleted). Thus, you must do all the steps of this procedure for each system that you want to configure using a USB key.

# 3.5 Unconfiguring a System

This procedure describes how to use the Configuration Utility to unconfigure Intel AMT on a system.

> **Note:**
>
> If the system was configured with Active Directory integration, the Configuration Utility does not delete the object representing the system. Delete the object manually.

### To unconfigure a system:

1. From the Configuration Options window, select **Unconfigure**. The Unconfigure System window opens.

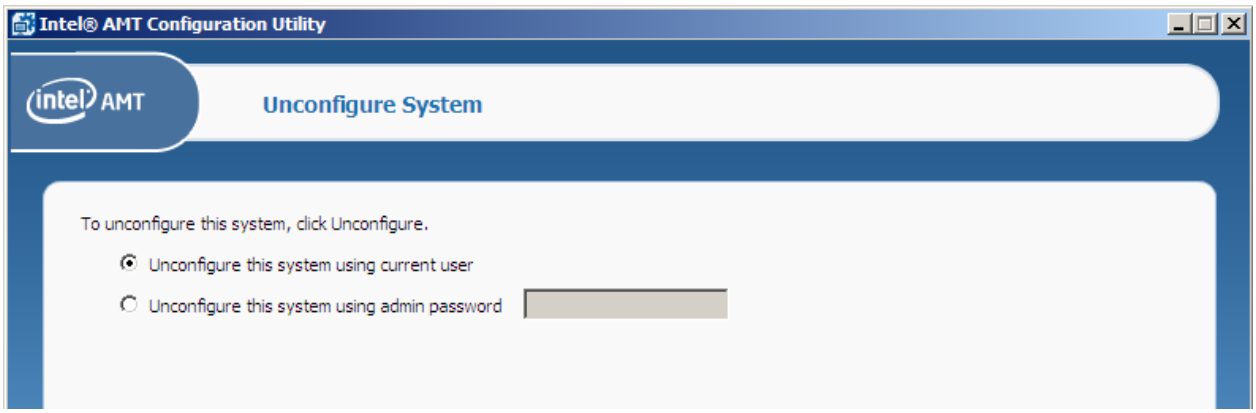



Figure 3-8: Unconfigure System Window

2. If the system is in Admin Control mode, you must select the user credentials to use during unconfiguration:
   - **Unconfigure this system using current user** – Select this option if the user running the Configuration Utility is defined in the Intel AMT device as an administrator.
   - **Unconfigure this system using admin password** – Select this option to unconfigure using the default admin user. You must supply the password of the admin user.

   > **Note:**
   >
   > If the system is in Client Control mode, this step is not required (the fields are not shown).

3. Click **Unconfigure**. The Configuration Utility deletes all the Intel AMT settings from the system and disables the Intel AMT features on the system.

# 3.6 Using the Profile Designer

The Profile Designer window lets you create profiles with configuration settings for multiple systems. These profiles are used by the Configurator. The location of the profiles is shown in the top left section ("Profiles Folder"). The right pane shows the configuration settings of the profile selected in the left pane.

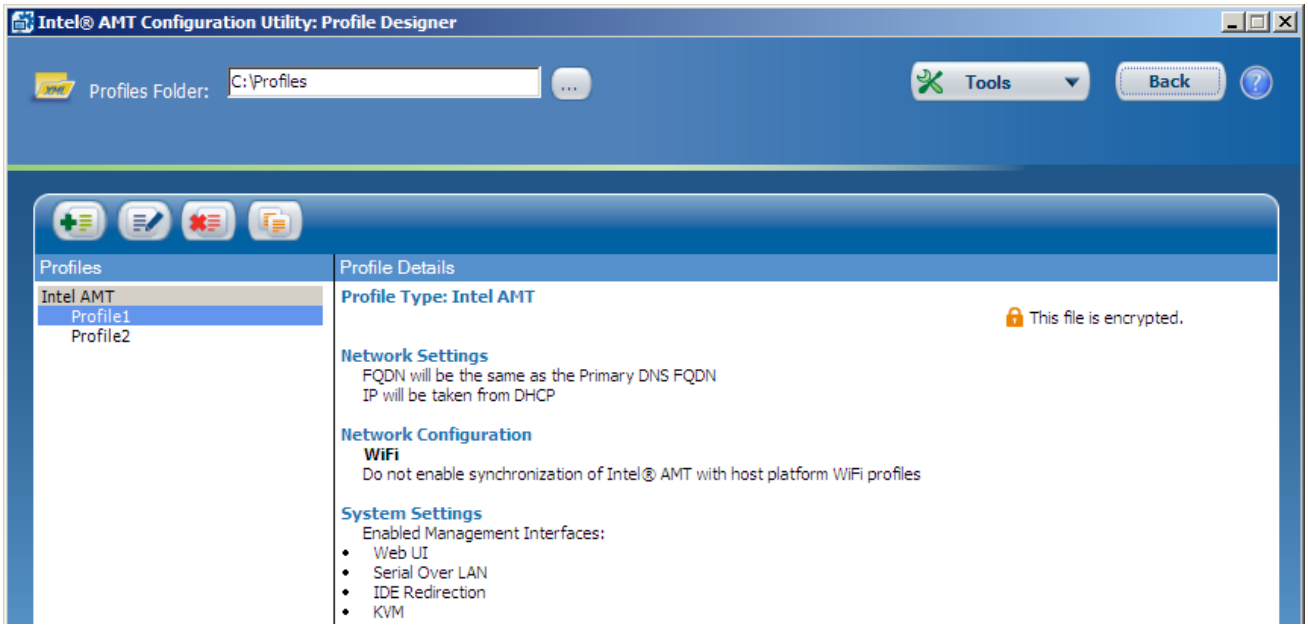



Figure 3-9: Profile Designer Window

This table describes the options available from the Profile Designer.

Table 3-1: Profile Designer Options

| Click | To do this... |
|---|---|
| | Define the folder where the profiles are located |
| | Create a new profile (see Creating a Configuration Profile for Intel AMT on page 44) |
| | Duplicate the profile selected in the left pane |
| | Delete the profile(s) selected in the left pane |
| | Edit the profile selected in the left pane |
| | Close the Profile Designer and go back to the Welcome window |
| | Create a USB key for manual configuration (see Defining Manual Configuration (Multiple Systems) on the next page) |

# 3.7 Defining Manual Configuration (Multiple Systems)

You can prepare a USB key with identical configuration settings to use with multiple Intel AMT systems. When the systems are rebooted with the USB key, Intel AMT is configured on them.

**Note:**

- This option is available only for systems with Intel AMT 6.0 and higher. For other Intel AMT systems you must prepare a new USB key for each system (see SMB/Manual Configuration on page 4).
- Intel SCS does not restrict the size of USB key you can use. But, the computer BIOS must fully support the selected USB key and be able to boot from it.

### To prepare the USB key:

1. Put a USB key in the computer.
2. From the Welcome window, click **Create Settings to Configure Multiple Systems**. The Profile Designer opens.
3. Select **Tools** > **Prepare a USB Key for Manual Configuration**. The Settings for Manual Configuration of Multiple Systems window opens.

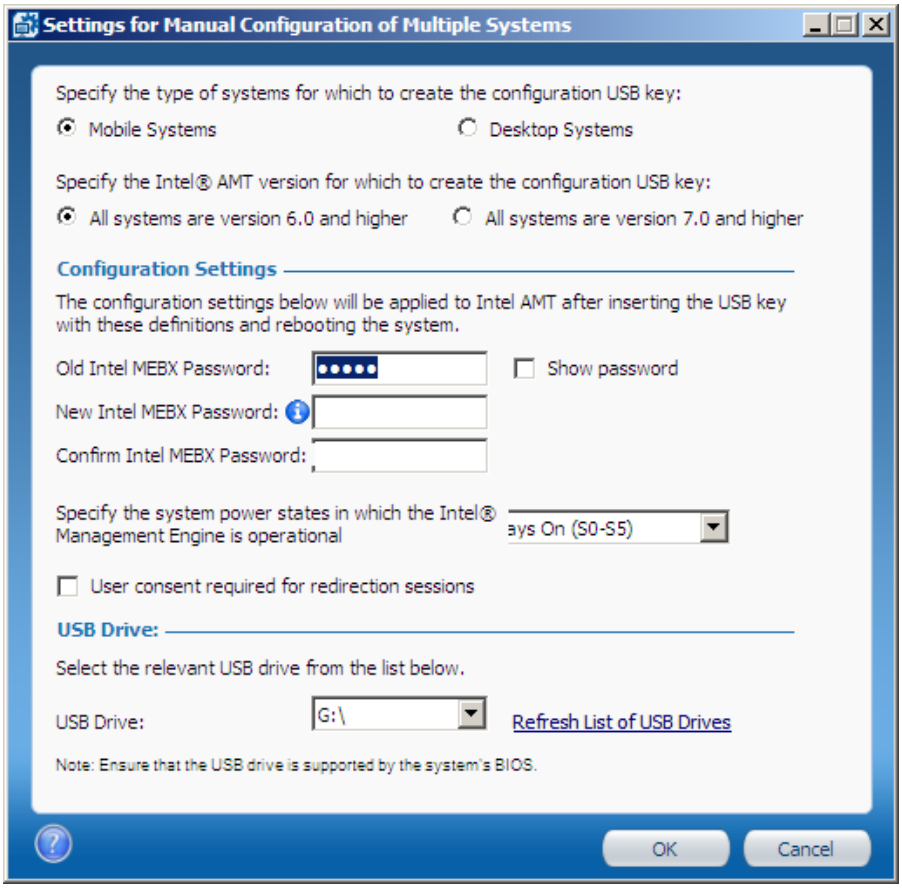



Figure 3-10: Settings for Manual Configuration of Multiple Systems Window

4. If you have mobile and desktop systems, you must prepare a different USB key for each type. This is because mobile and desktop systems have different power settings. Select the type of system that this USB key will configure:
   - **Mobile Systems**
   - **Desktop Systems**
5. Select the versions of Intel AMT that this USB key will configure:
   - **All systems are version 6.0 and higher** – If selected, you can use this USB key to configure all systems that have Intel AMT 6.x and higher.
   - **All systems are version 7.0 and higher** – If selected, you can use this USB key to configure only systems that have Intel AMT 7.x. and higher. The data in the USB key is "scrambled" so it cannot easily be read.

   **Note:**

   Make sure that you keep this USB key in a secure location. The data in the USB key is NOT encrypted (even if it is "scrambled").
6. In the Configuration Settings section, enter the password for the Intel MEBX:
   - **Old Intel MEBX Password** – Intel SCS always puts the default password of unconfigured systems ("admin") in this field. If this is not the password currently defined in the Intel MEBX, enter the correct password. If you do not supply the correct password, configuration will fail.
   - **New Intel MEBX Password** – The new password to put in the Intel MEBX. For the first configuration it is mandatory to change the password. For reconfiguration you must also enter a value here, but it can be the same as the Current Password.

     For information about the required format, see Password Format on page 5.
7. From the drop-down list, define in which power states (of the host system) the Intel AMT device will operate:
   - **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.
8. (Optional) By default, the user consent feature is not enabled for systems configured using this configuration method (see User Consent on page 8). If you want to define that user consent is mandatory for redirection sessions, select **User consent required for redirection sessions**.
9. From the USB Drive drop-down list, select the drive letter of the USB key (you cannot select a USB key if you are using it to run the Console).
10. Click **Next**. The Formatting USB drive window opens.
11. Click **Yes** if you are sure you want to continue and format the USB key. After formatting completes, Intel SCS creates the configuration file on the USB key.

# Chapter 4

## 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:


4.1 About Intel AMT Profiles ..... 43
4.2 Creating a Configuration Profile for Intel AMT ..... 44
4.3 Defining the Profile Scope ..... 47
4.4 Defining Profile Optional Settings ..... 48
4.5 Defining Active Directory Integration ..... 49
4.6 Defining the Access Control List (ACL) ..... 52
4.7 Defining Home Domains ..... 56
4.8 Defining Remote Access ..... 57
4.9 Defining Trusted Root Certificates ..... 61
4.10 Defining Transport Layer Security (TLS) ..... 63
4.11 Defining Network Setups ..... 66
4.12 Defining System Settings ..... 75

# 4.1 About Intel AMT Profiles

Configuration profiles created by the Configuration Utility are in XML format. Configuration profiles contain the settings that will be put into the Intel AMT devices during configuration using the Configuration Utility/Configurator.

You can also create Delta Profiles that 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:**

Profiles created using the Configuration Utility can only be used with the Host-based Configuration method (supported from Intel AMT 6.2 and higher).

# 4.2 Creating a Configuration Profile for Intel AMT

The Configuration Profile Wizard lets you create and edit configuration profiles. This wizard starts when you:

- Click **Edit Configuration** in the Configure via Windows window (see Configuring a System on page 30)
- Click or in the Profile Designer window (see Using the Profile Designer on page 39)

When you start the Configuration Profile Wizard, the Getting Started window opens.

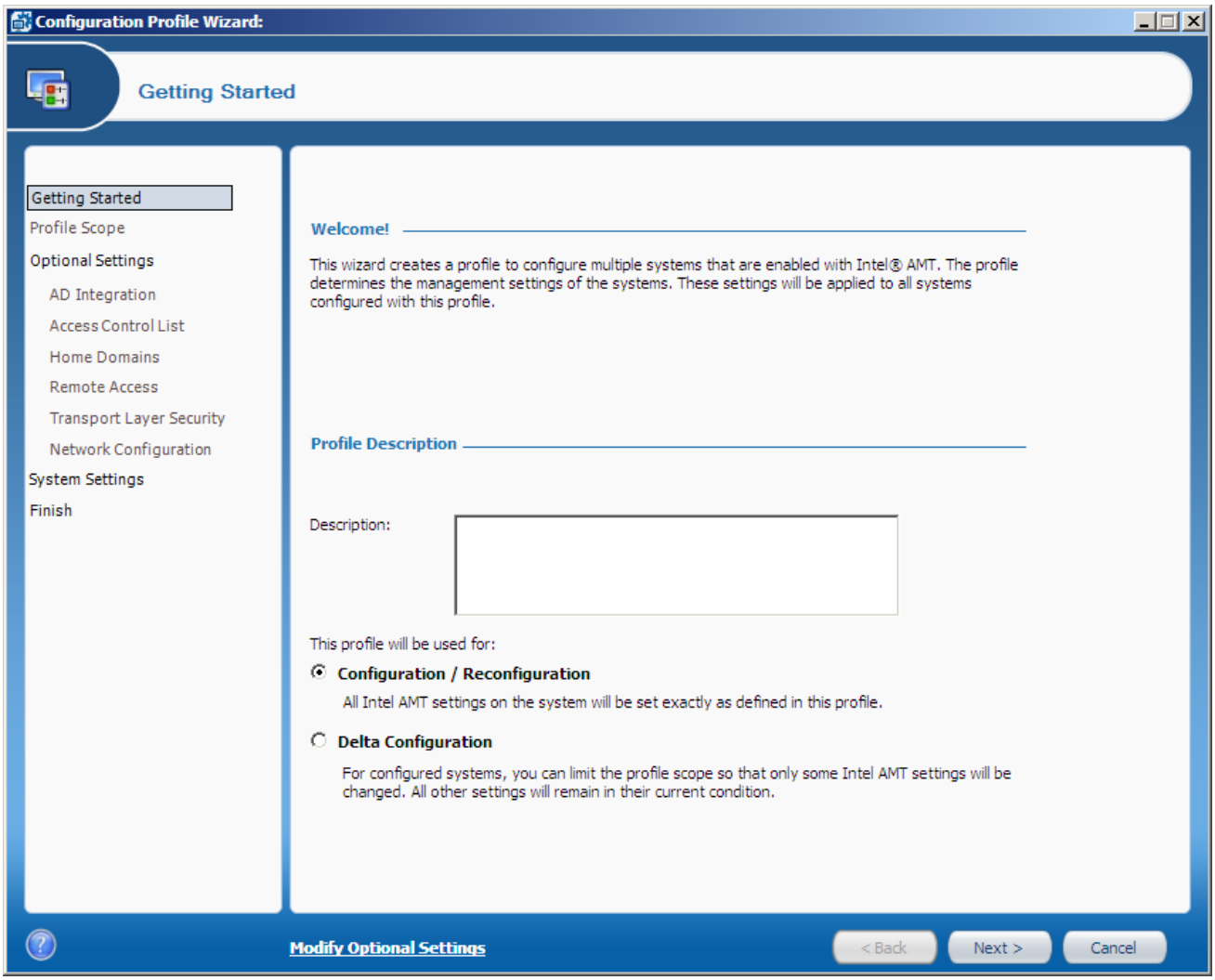



Figure 4-1: Getting Started Window

### To create a configuration profile for Intel AMT:

1. (Optional) In the Description field, enter a description for the profile. This field is for informational purposes only.

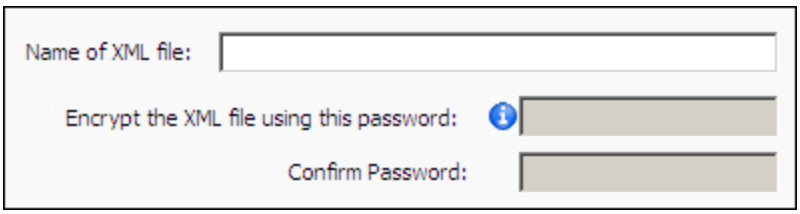
2. Select the task for which you want to use this profile:
   - **Configuration / Reconfiguration** – Systems configured using this profile will be set with the Intel AMT settings exactly as they are defined in this profile. Optional settings that are not defined in this profile will be removed from 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.
3. Click **Next** to continue in the Configuration Profile Wizard and define the settings as described in these topics:
   - Defining the Profile Scope on page 47
   - Defining Profile Optional Settings on page 48
     - Defining Active Directory Integration on page 49
     - Defining the Access Control List (ACL) on page 52
     - Defining Home Domains on page 56
     - Defining Remote Access on page 57
     - Defining Transport Layer Security (TLS) on page 63
     - Defining Network Setups on page 66
   - Defining System Settings on page 75
4. When you have defined all the required settings for this profile, save the profile (see Saving the Configuration Profile below).

## 4.2.1 Saving the Configuration Profile

The Finish window is the last step when you create a new profile or edit an existing profile. The type of profile and the settings you define in the profile cause different fields to show in the Finish window.

### To save the profile:

1. When you create or edit a profile in the Profile Designer, these fields are shown:



a. In the Name of XML file field, enter a name for this profile. The profile name:

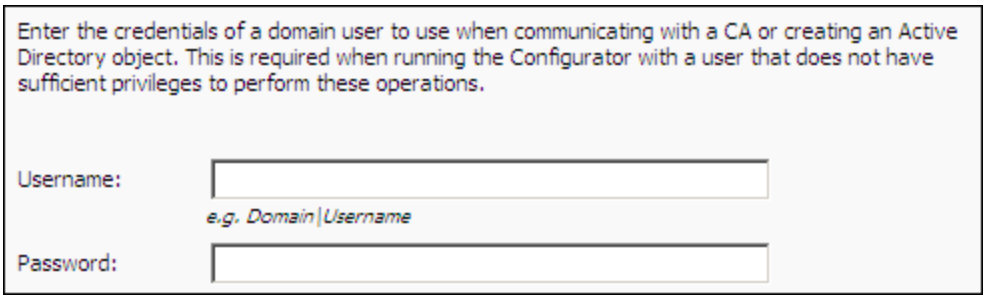
- Can be a maximum of 32 characters
- Cannot be empty or include only "whitespace" characters
- Must include only 7-bit ASCII characters in the range of 32-126, not including these characters: ( / ), ( \ ), ( : ), ( * ), ( ? ), ( < ), ( > ), ( . ), ( , ), ( & ), ( " ), ( ' ), ( | )

b. In the password fields, enter a password that will be used to encrypt the profile. For information about the required format, see Password Format on page 5.

> **Note:**
>
> Remember this password. You will need to supply it each time you want view, edit, or use this profile.

2. If the profile includes any of these settings:
   - Active Directory Integration
   - Requesting certificates from a Certification Authority

   these optional fields are shown:




   Make sure that the Configuration Utility runs under a user with permissions to communicate with the CA or create Active Directory objects. On operating systems with User Account Control (UAC), the local administrator account does not have sufficient permissions. If you supply a username and password here, the Configuration Utility uses them to do these tasks.

3. Click **Finish**.

# 4.3 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

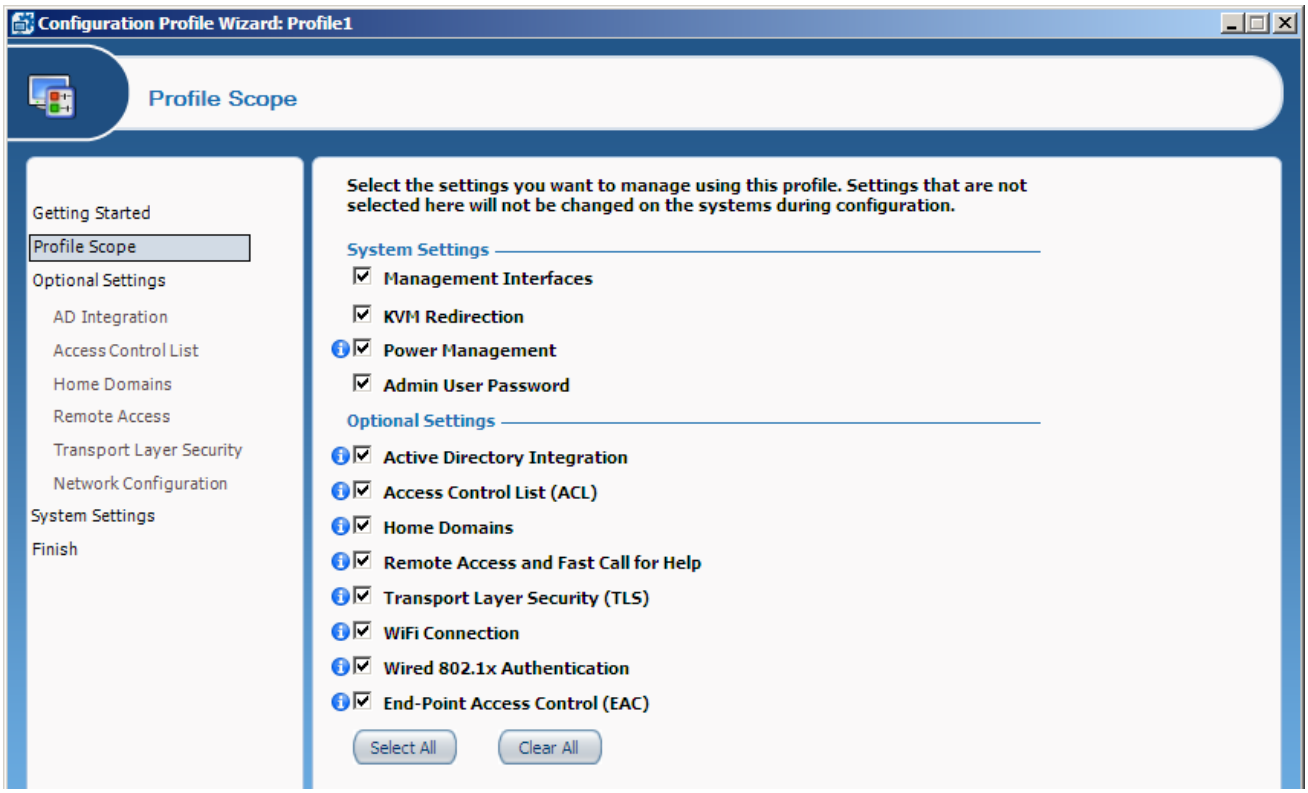



Figure 4-2: Profile Scope Window

### 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.

# 4.4 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.

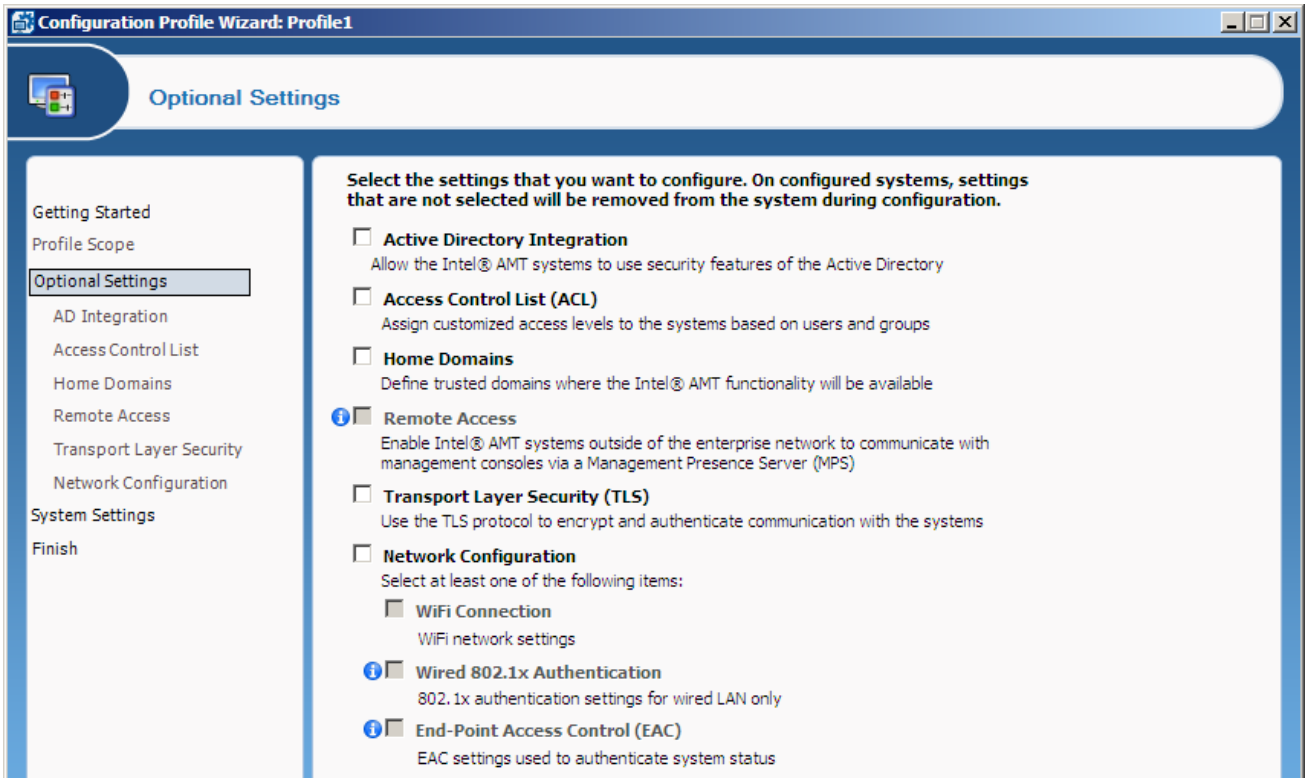



Figure 4-3: Profile Optional Settings Window

### 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 52
   - Defining Home Domains on page 56
   - Defining Remote Access on page 57
   - Defining Transport Layer Security (TLS) on page 63
   - Defining Network Setups on page 66

# 4.5 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)

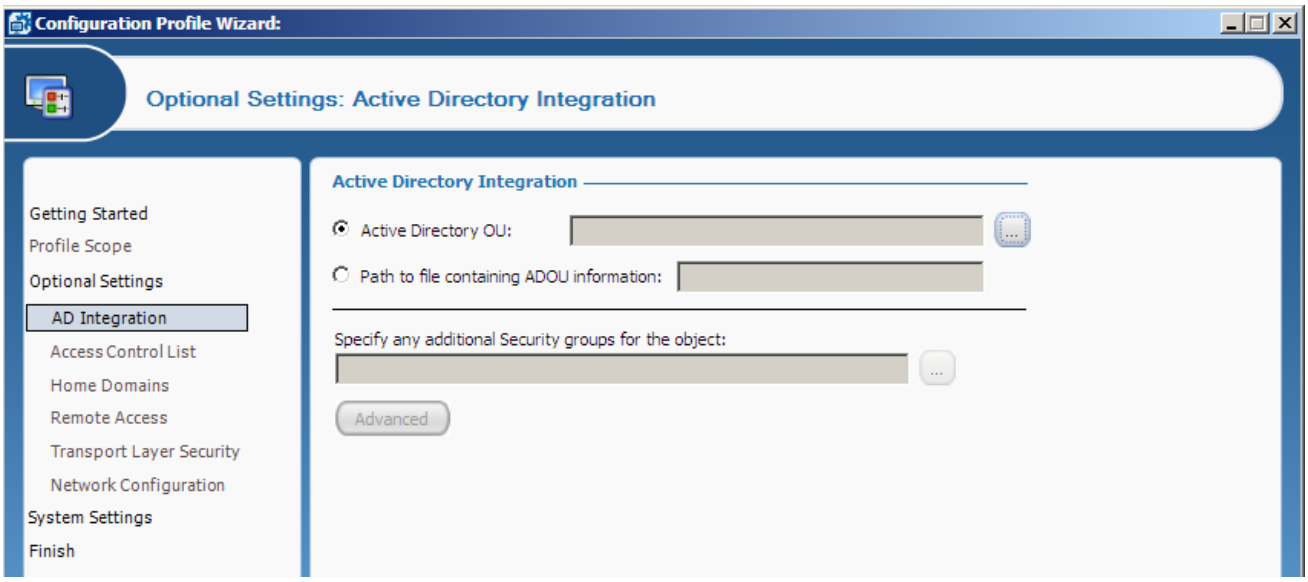



Figure 4-4: Active Directory Integration Window

### To define Active Directory Integration:

Select one of these options:

- **Active Directory OU -**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.
- **Path to file containing ADOU information** – This is an advanced option, not necessary in most network environments, and requires knowledge about creating AD objects. Before you can use this option, you must manually create an object for the Intel AMT device. For more information, refer to the `ADObjectFile.xml` example in the `sample_files` folder.

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.

For more information about the remaining optional settings, see:

- Defining Additional Security Groups on the next page
- Defining Additional Object Attributes on page 51

## 4.5.1 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.

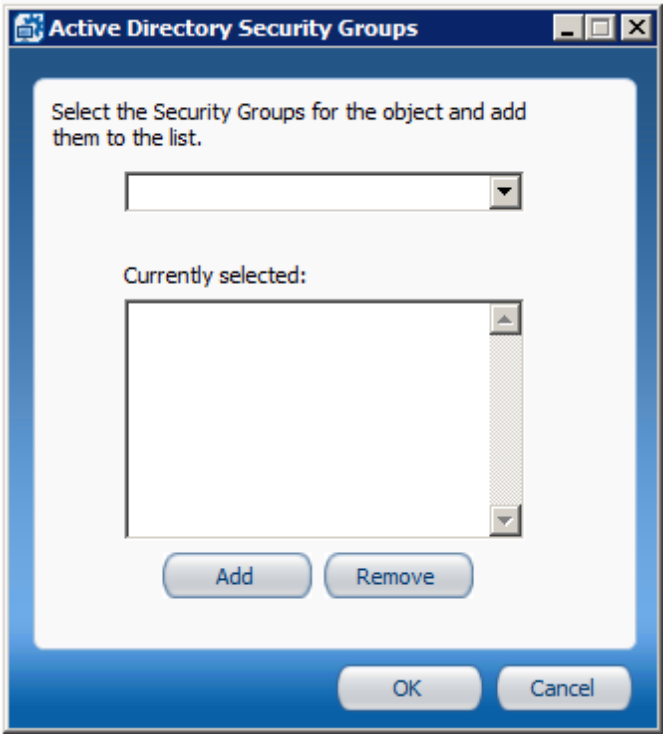



Figure 4-5: Active Directory Security Groups Window

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.

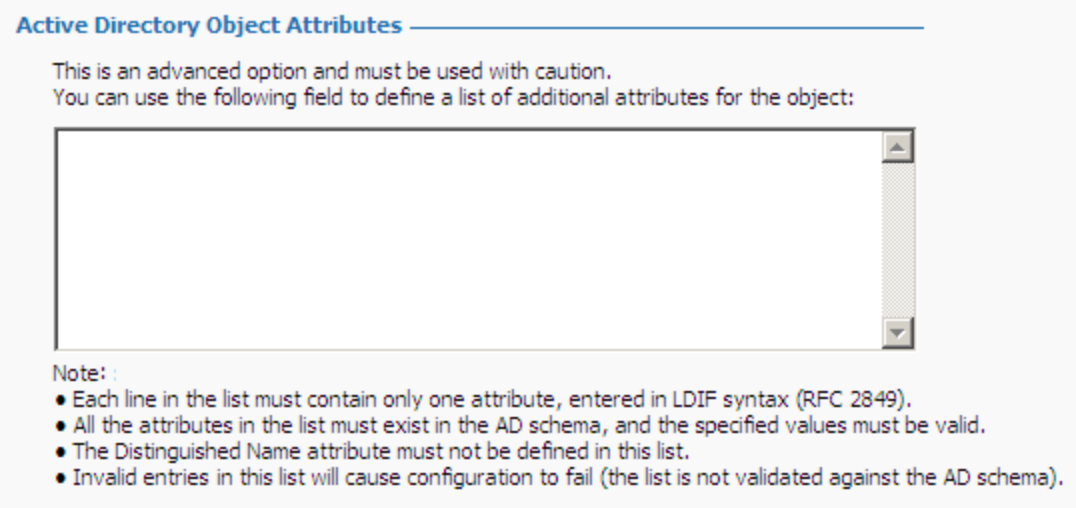
## 4.5.2 Defining Additional Object Attributes

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.

# 4.6 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 4-6: 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.

## 4.6.1 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.

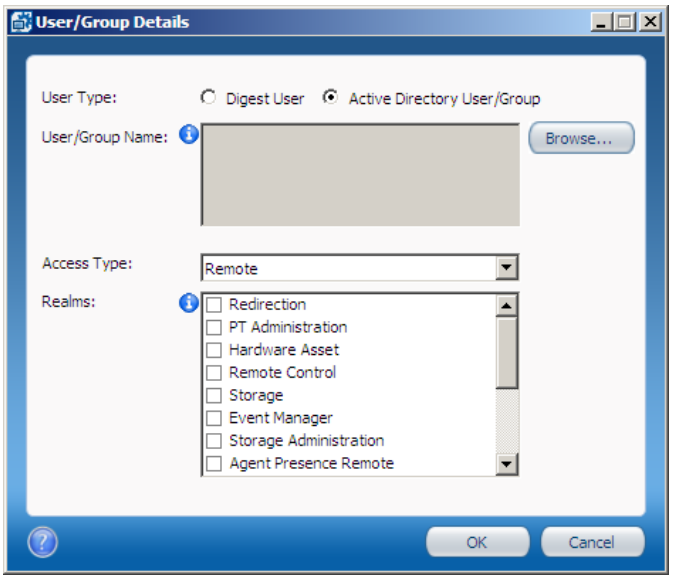



Figure 4-7: User/Group Details Window

2. In the User Type section, select the required type of user:
   - **Digest User** – Enter the username and password (see Password Format on page 5). 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 4-1: 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.<br>**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 |

## 4.6.2 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.

**Note:**

The Access Monitor feature is available from Intel AMT 4.0 and higher.

# 4.7 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.

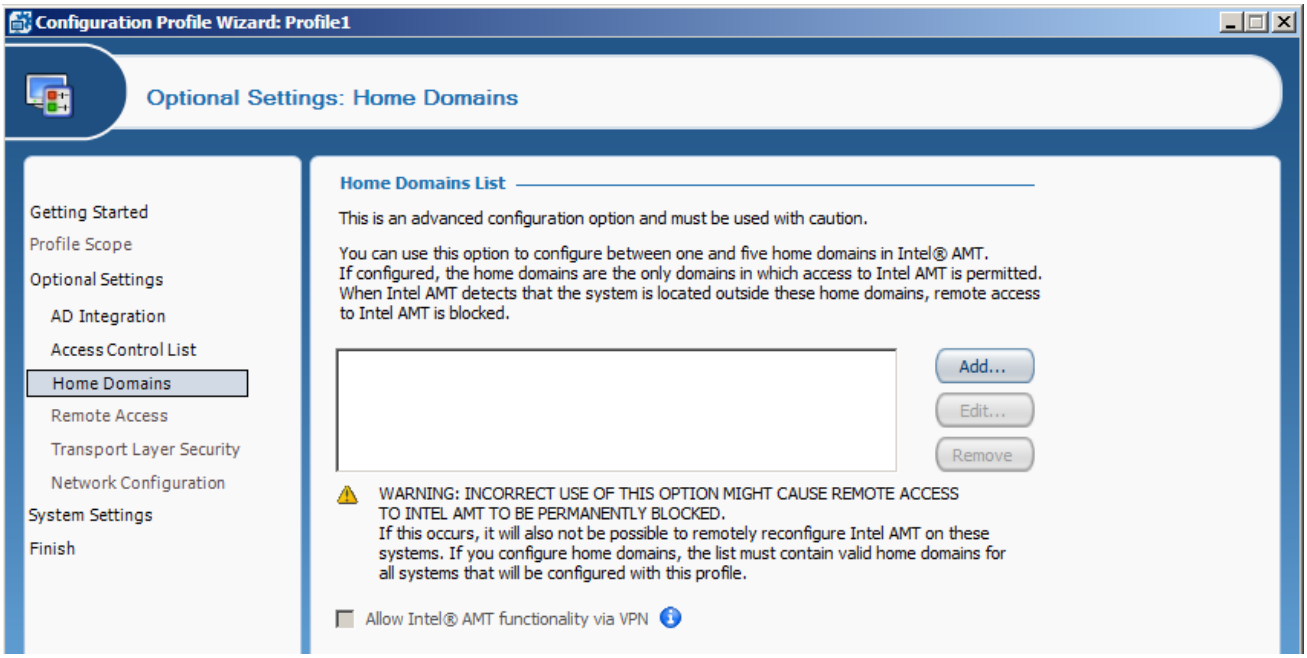



Figure 4-8: Home Domains Window

### 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.

# 4.8 Defining Remote Access

The remote access feature lets Intel AMT systems (versions 4.x and higher) 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.

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.

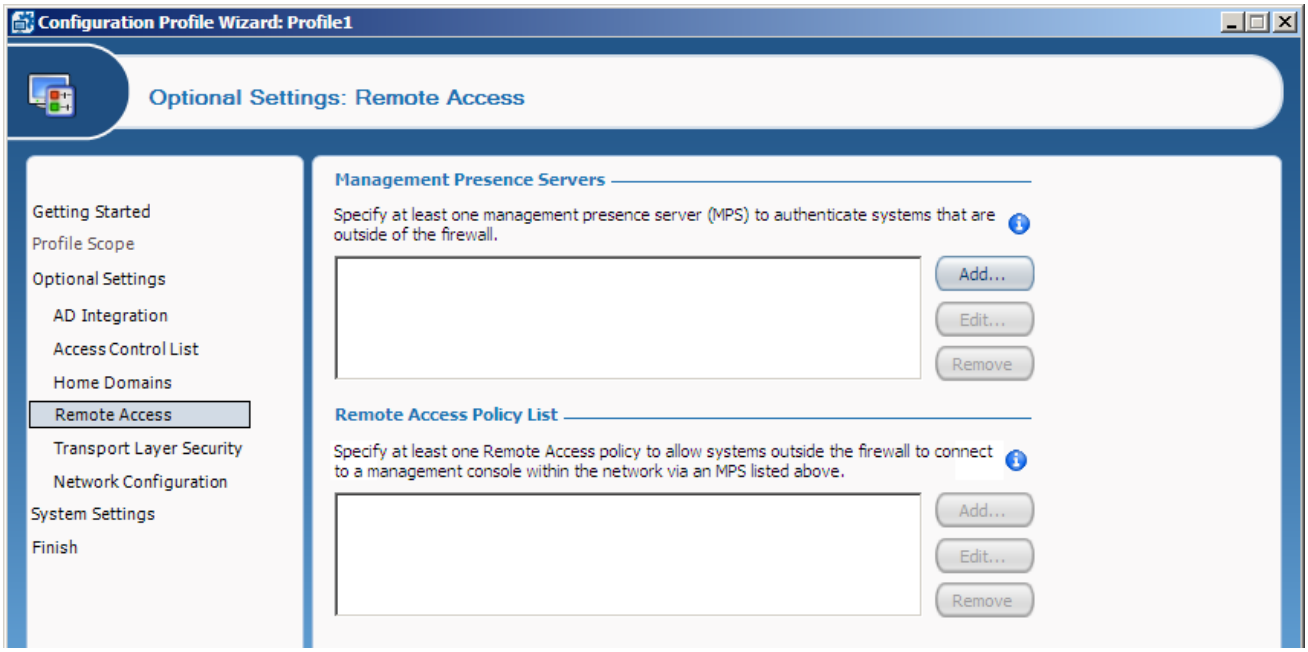



Figure 4-9: Remote Access Window

To define the remote access parameters, see these topics:

- Defining Management Presence Servers on the next page
- Defining Remote Access Policies on page 60

## 4.8.1 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.

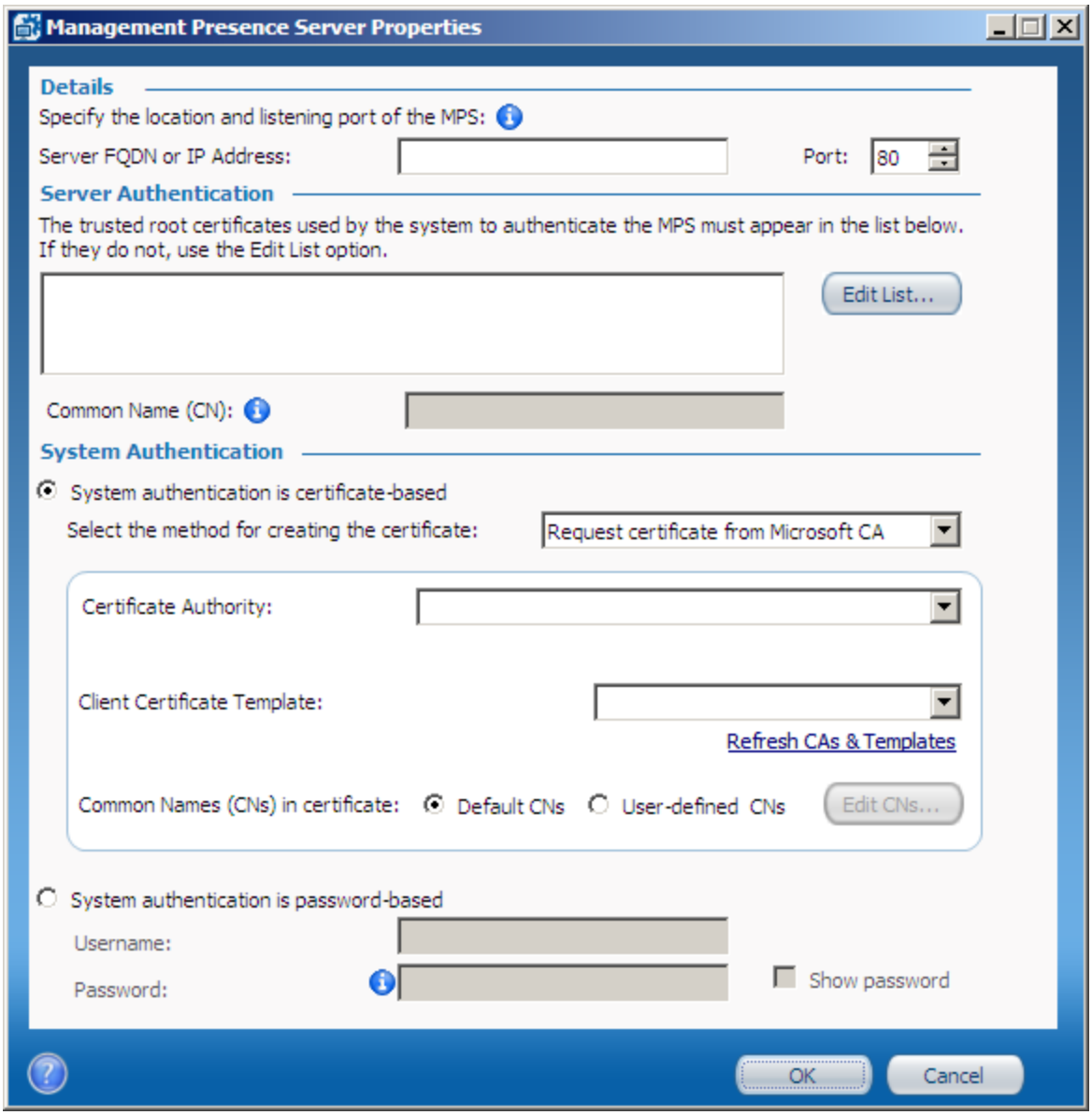



Figure 4-10: Management Presence Server Properties Window

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 Certificates on page 61).
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 from step 8.
   - **Use certificate from a file** – For information about this method and the necessary file format, see Using Predefined Files Instead of a CA Request on page 113. If you select this option, define the file locations 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 107.
   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 114.

   **Note:**

   - To use this option, Intel SCS must have access to the CA during configuration (see Required Permissions on the CA on page 105).
   - 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.

## 4.8.2 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.

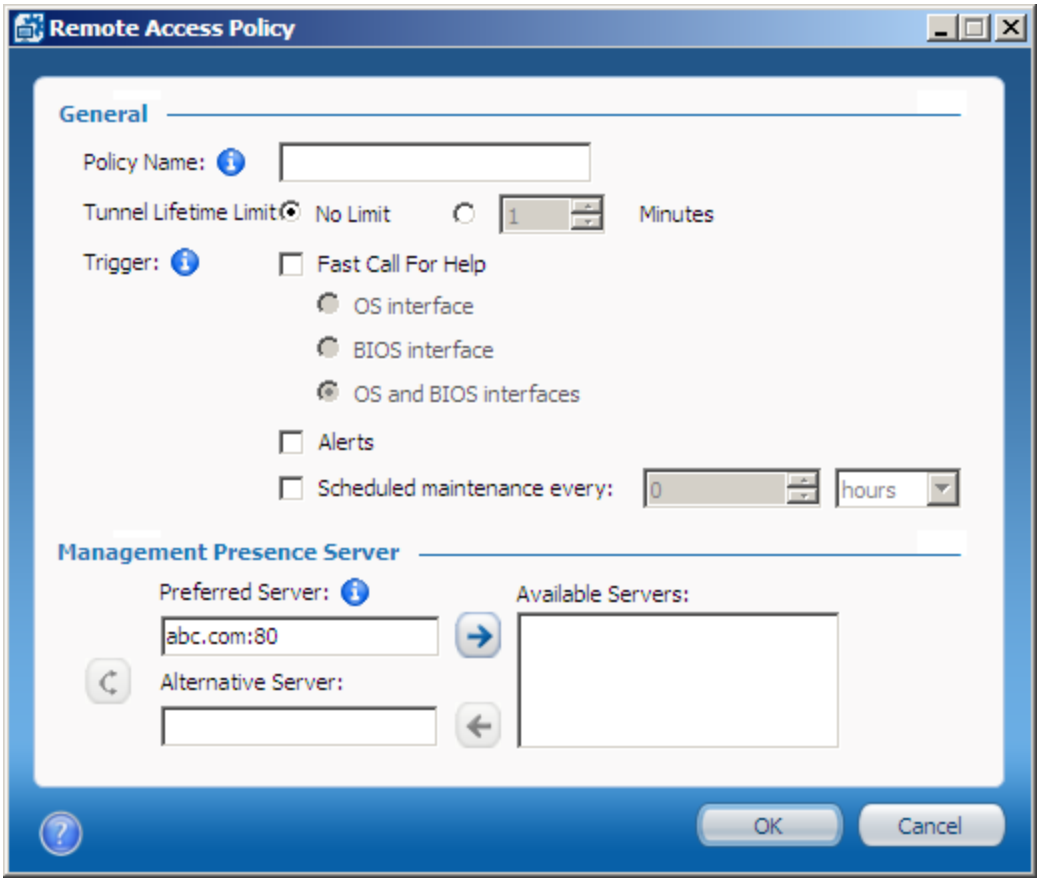



Figure 4-11: Remote Access Policy Window

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.

# 4.9 Defining Trusted Root Certificates

An Intel AMT system must have a trusted root certificate 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.

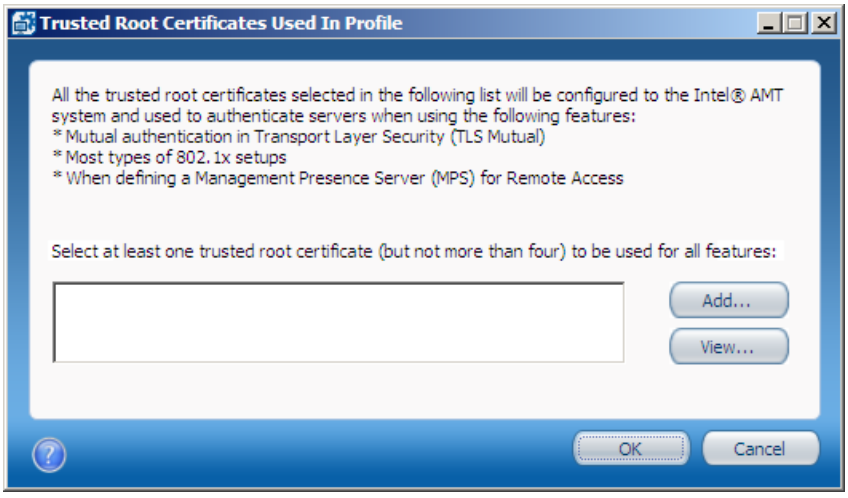



Figure 4-12: Trusted Root Certificates Used In Profile Window

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

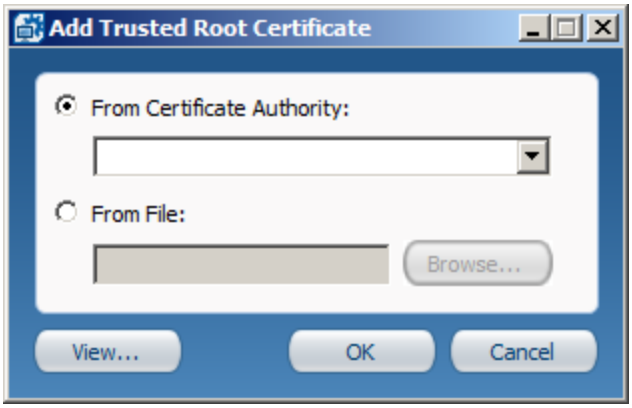



Figure 4-13: Add Trusted Root Certificate Window

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

> **Note:**
>
> You can only add a certificate from a CA if the certificate is self-signed and the CA is a root CA. You cannot add a certificate from a subordinate CA.

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.

# 4.10 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. 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.

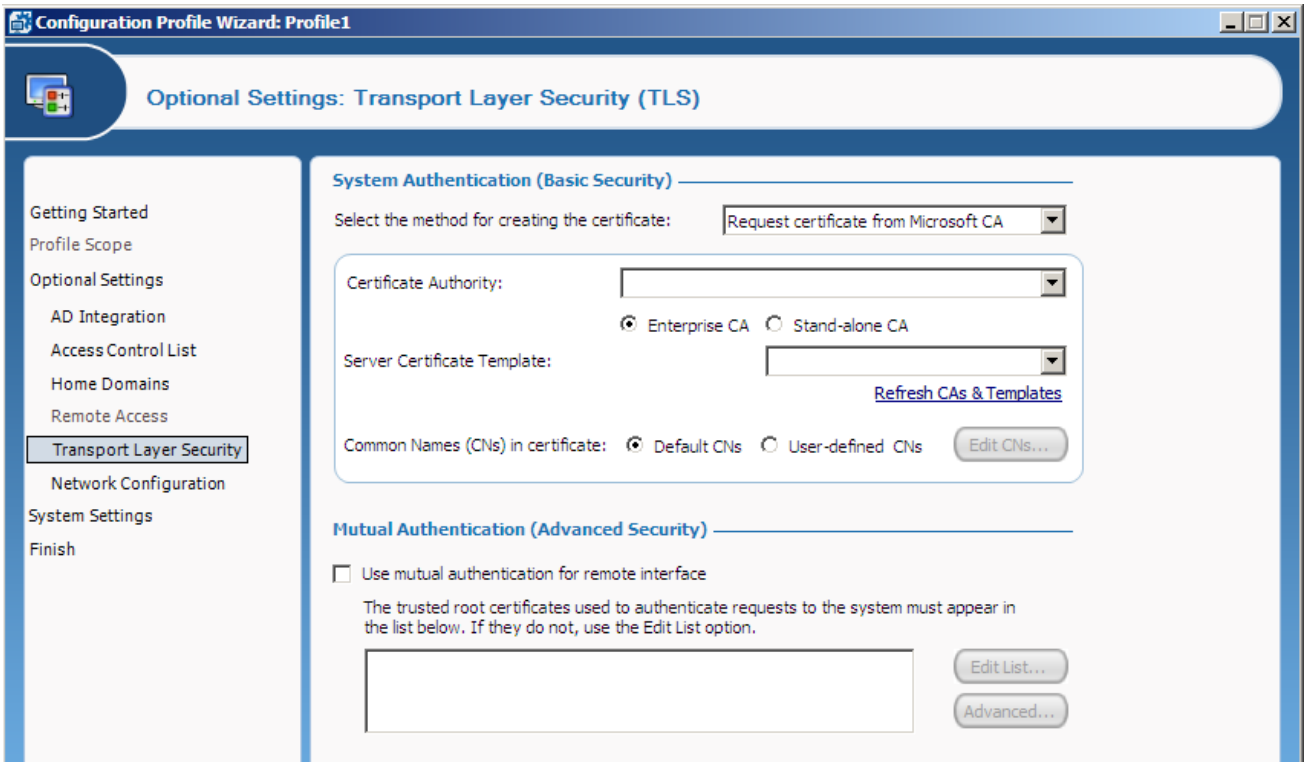



Figure 4-14: Transport Layer Security (TLS) Window

**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 from step 2.
   - **Use certificate from a file** – For information about this method and the necessary file format, see Using Predefined Files Instead of a CA Request on page 113. If you select this option, define the file locations 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 root CA or an Enterprise root CA.

   b. If you are using an Enterprise root 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 107.

   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 114.

   **Note:**

   - To use this option, Intel SCS must have access to the CA during configuration (see Required Permissions on the CA on page 105).
   - 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 Certificates on page 61).

   c. (Optional) Define advanced mutual TLS settings (see Defining Advanced Mutual Authentication Settings below).

## 4.10.1 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 116 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.

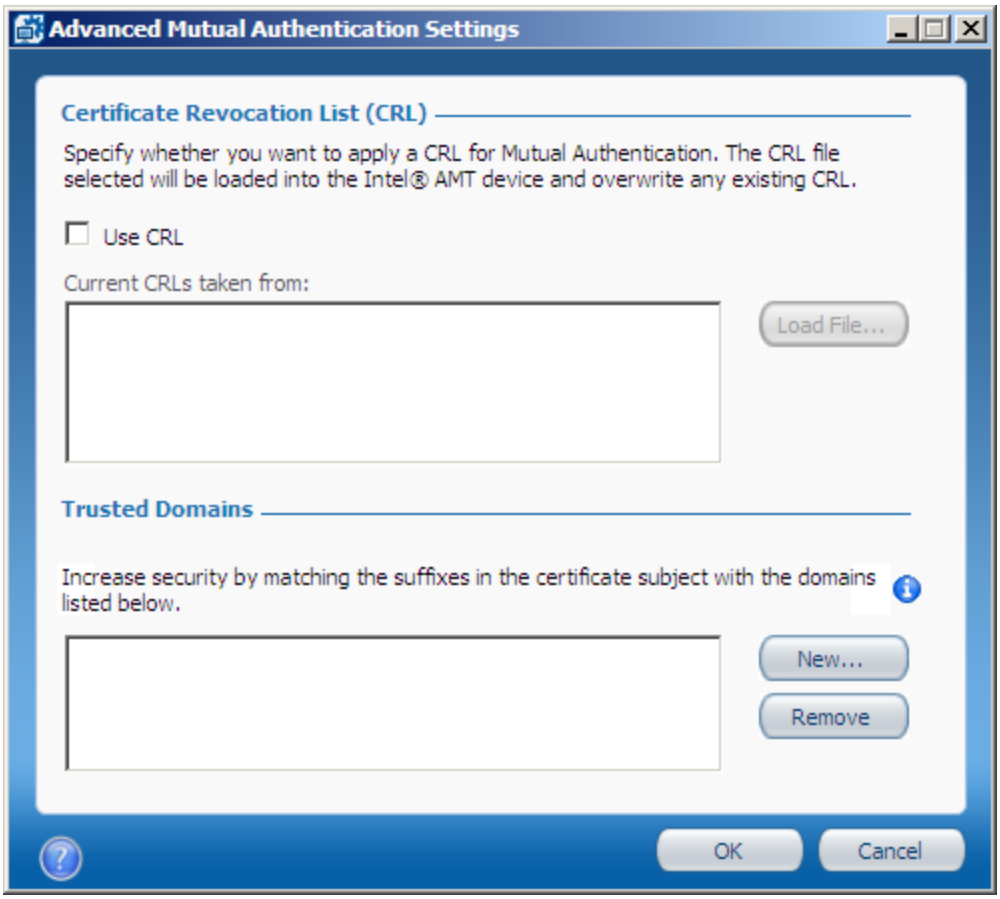



Figure 4-15: Advanced Mutual Authentication Settings Window

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.

# 4.11 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 126.

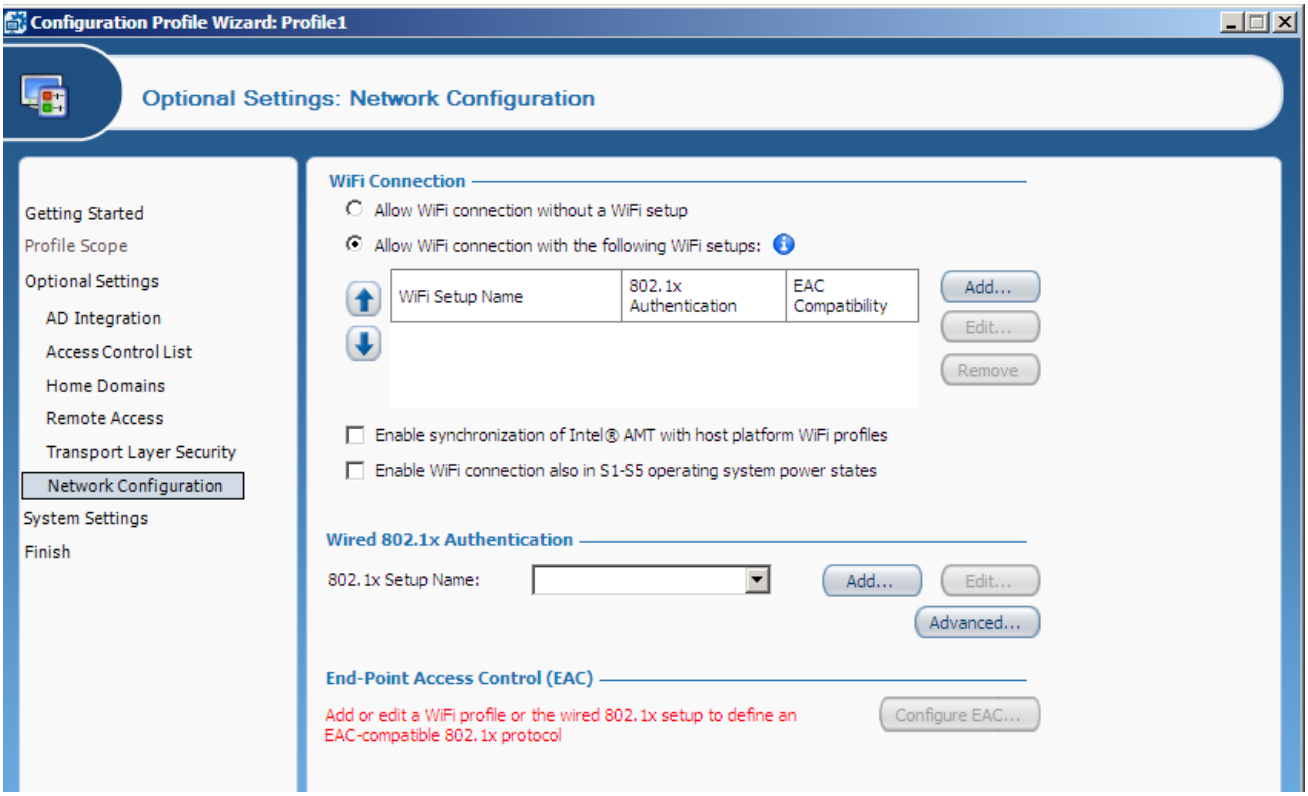



Figure 4-16: Network Configuration Window

### 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 70).

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

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

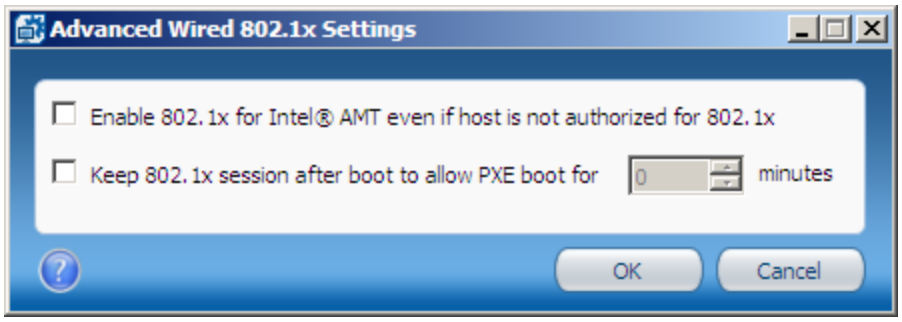



   Figure 4-17: Advanced Wired 802.1x Settings Window

   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 73).

## 4.11.1 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 WiFi 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.

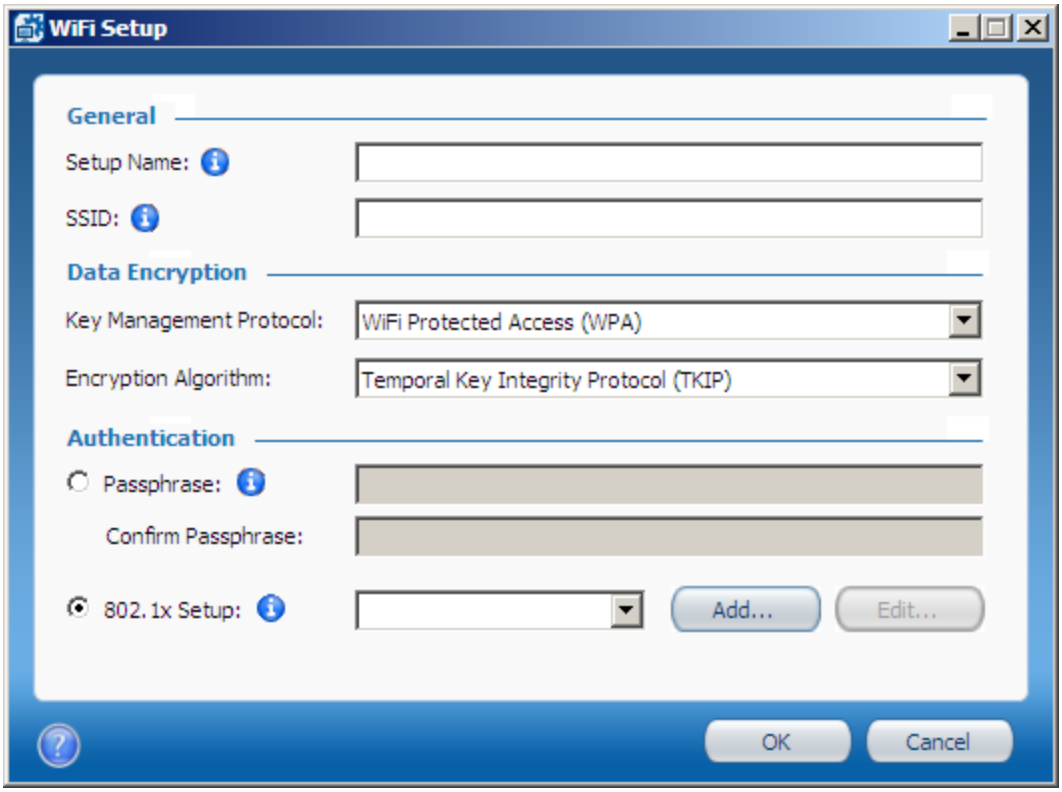



Figure 4-18: WiFi Setup Window

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. If left empty, the device will try to connect to all WiFi networks that use Data Encryption as defined in this WiFi Setup.
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.

## 4.11.2 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 49) 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.

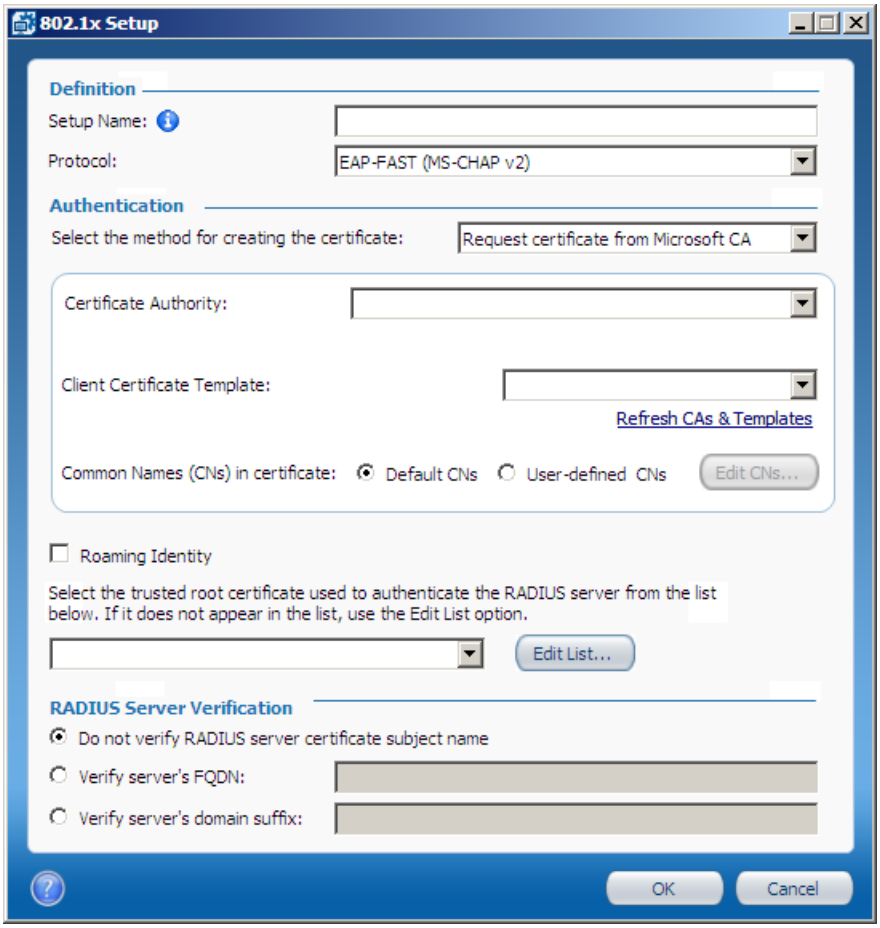



Figure 4-19: 802.1x Setup Window

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 4-2: 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.
   - **Use certificate from a file** – For information about this method and the necessary file format, see Using Predefined Files Instead of a CA Request on page 113. If you select this option, define the file locations 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 107.
   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 114.

   **Note:**

   - To use this option, Intel SCS must have access to the CA during configuration (see Required Permissions on the CA on page 105).
   - 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 Certificates on page 61). 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.

## 4.11.3 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 49) 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.

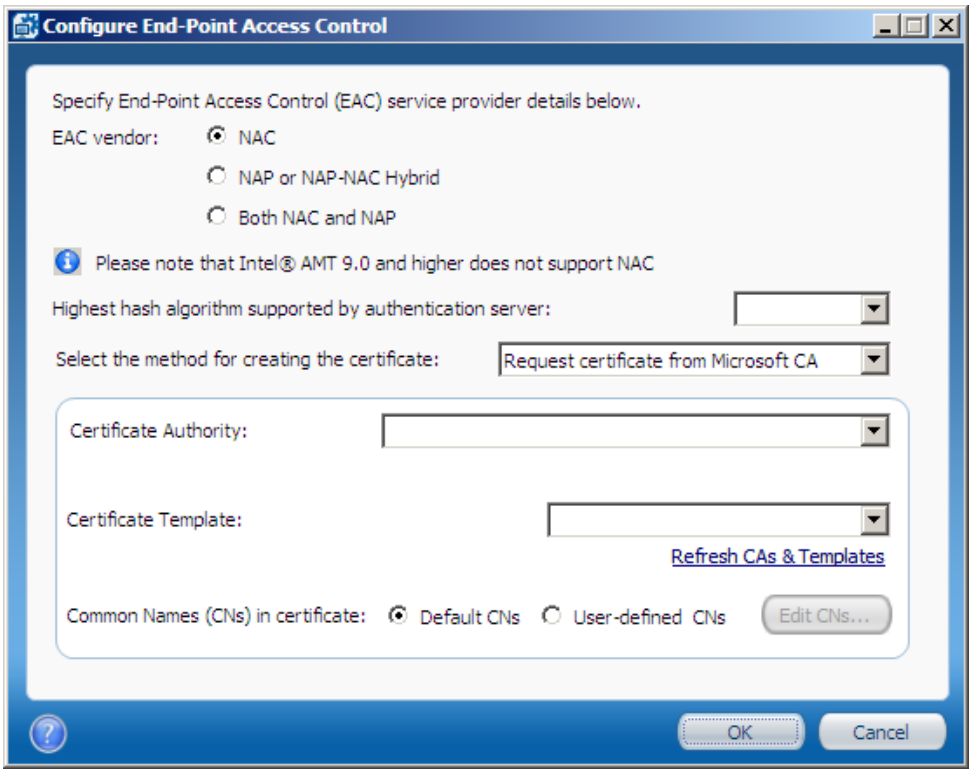



Figure 4-20: Configure End-Point Access Control Window

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.
   - **Use certificate from a file** – For information about this method and the necessary file format, see Using Predefined Files Instead of a CA Request on page 113. If you select this option, define the file locations 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 107.
   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 114.

   **Note:**

   - To use this option, Intel SCS must have access to the CA during configuration (see Required Permissions on the CA on page 105).
   - 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.

# 4.12 Defining System Settings

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

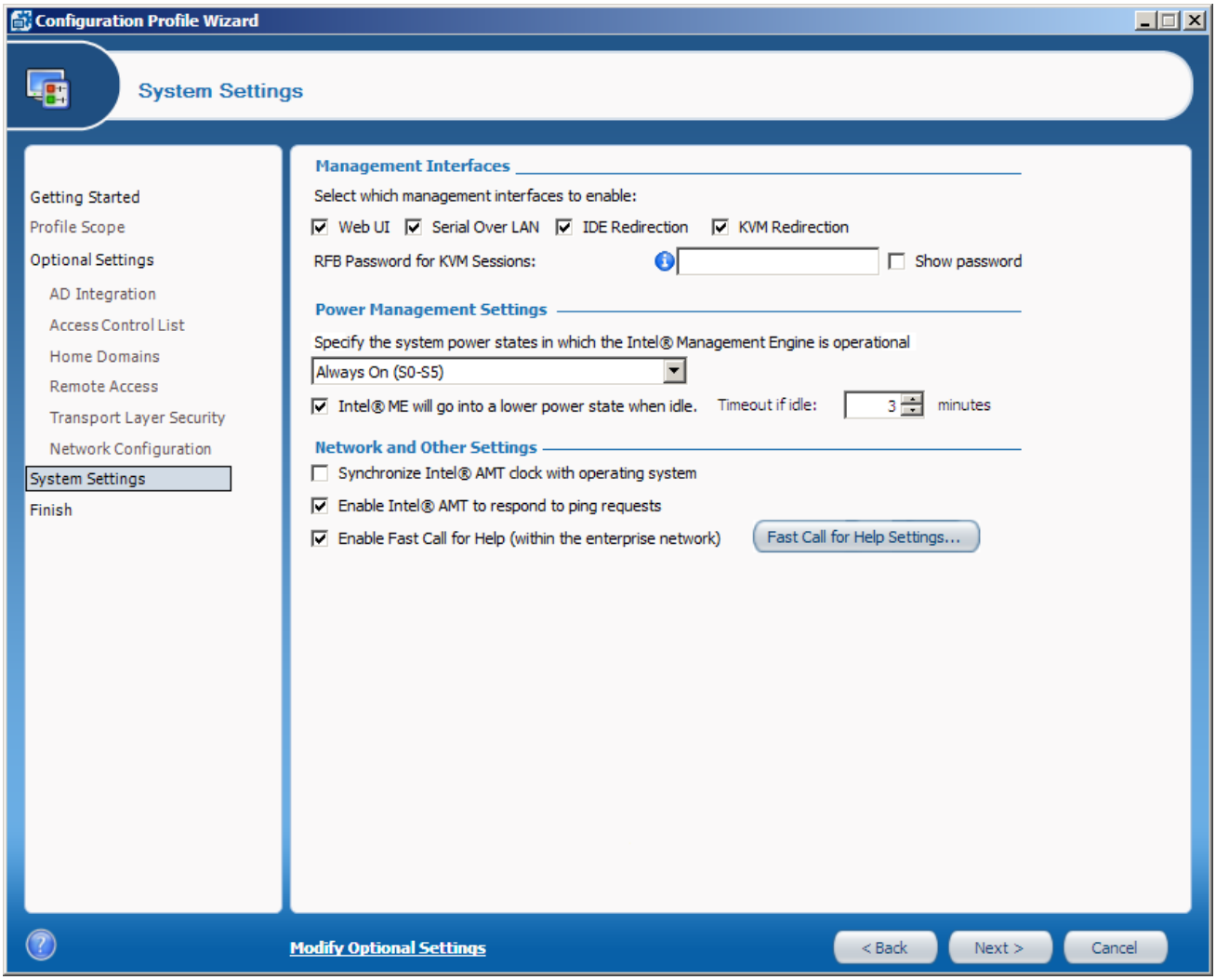



Figure 4-21: System Settings Window

> **Note:**
>
> The location in the Configuration Utility from where you open the Configuration Profile Wizard causes different options to show in the System Settings window.

For information about these settings, see:

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

## Management Interfaces

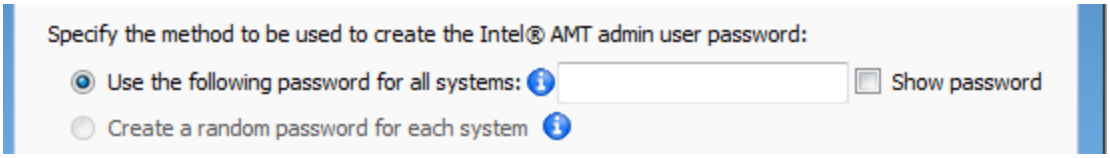
1. Select the interfaces you want to open on the Intel AMT system:
   - **Web UI** – Enables you to manage and maintain Intel AMT systems using a browser-based interface.
   - **Serial Over LAN** – Enables you to remotely manage Intel AMT systems by encapsulating keystrokes and character display data 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.
   - **KVM Redirection** – Opens the KVM Redirection interface. For more information about KVM, see Support for KVM Redirection on page 16.
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 16). If you enter a password, it must be EXACTLY eight characters (see Password Format on page 5).

## 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. When you edit a profile for multiple systems, these additional fields are shown:




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 5) 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.

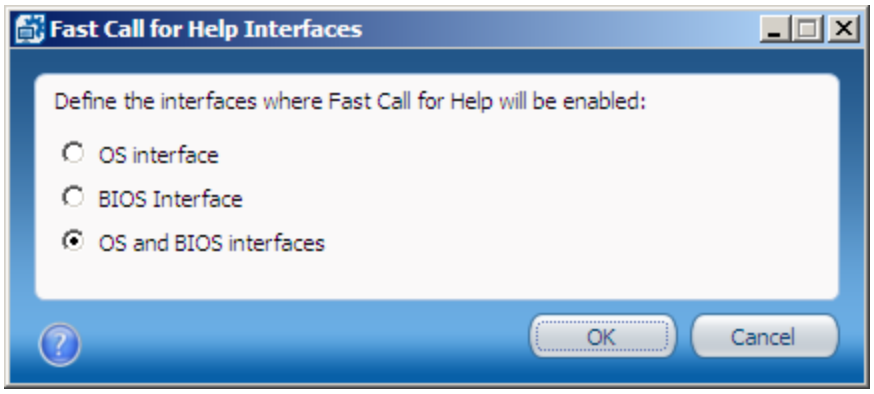
> **Note:**
>
> For important information about these password options (see Admin Permissions in the Intel AMT Device on page 10).

2. (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.

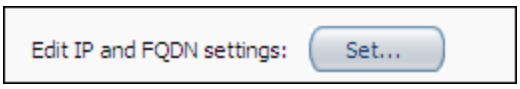
3. (Optional) **Select Enable Intel® AMT to respond to ping requests**. When this check box is selected, the Intel AMT device will respond to a ping if the host platform does not respond.
4. (Optional) You can define which interfaces are open for the local Fast Call for Help feature. If the computer 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 57.

5. When you edit a profile for multiple systems, this additional field is shown in the Network Settings section:




(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.

## 4.12.1 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.

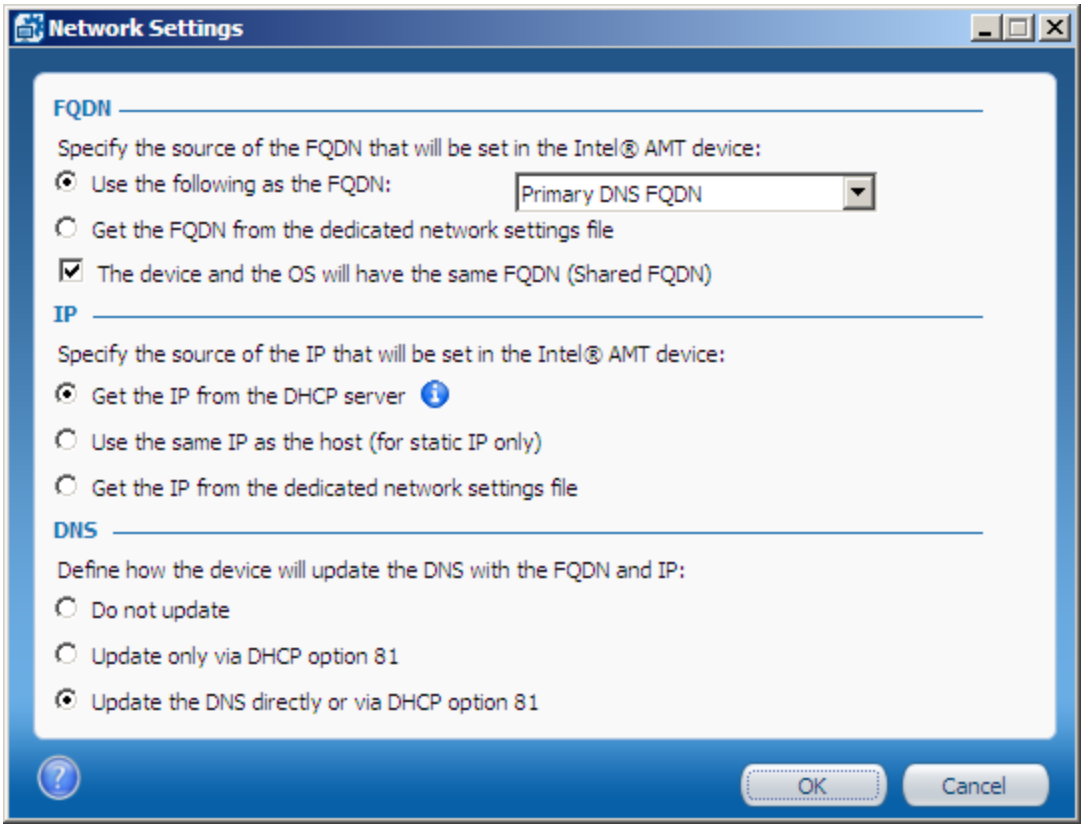



Figure 4-22: Network Settings Window

### 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 5

## Using the Configurator

This chapter describes how to use the Configurator.

For more information, see:


5.1 About the Configurator ..... 82
5.2 CLI Syntax ..... 82
5.3 Configurator Log Files ..... 83
5.4 CLI Global Options ..... 83
5.5 Verifying the Status of Intel AMT ..... 84
5.6 Discovering Systems ..... 84
5.7 Configuring Systems ..... 86
5.8 Configuring a System using a USB Key ..... 87
5.9 Maintaining Configured Systems ..... 90
5.10 Unconfiguring Intel AMT Systems ..... 92
5.11 Running Scripts with the Configurator ..... 95
5.12 Configurator Return Codes ..... 99

# 5.1 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.

The Configurator (`ACUConfig.exe`) is located in the Configurator folder.

**Note**

The Configurator folder also contains dll files that are necessary for the Configurator to operate.

# 5.2 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>.

**Note**

This guide only includes commands related to the configuration methods that are supported by the Configuration Utility. The syntax and descriptions of the commands in this guide include only the parameters that are supported by the Configuration Utility. For information about the full list of commands and parameters, supported by Intel SCS refer to the `Intel(R)_SCS_User_Guide.pdf`.

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.

# 5.3 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.

# 5.4 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 6.
- `/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`.

# 5.5 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 |

# 5.6 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.<br>If saved in the registry, the data is saved in each system at this location:<br>• 32-bit and 64-bit operating systems: `HKLM\SOFTWARE\Intel\Setup and Configuration Software\SystemDiscovery`<br>• In addition, on 64-bit operating systems: `HKLM\SOFTWARE\Wow6432Node\Intel\Setup and Configuration Software\SystemDiscovery`<br>Intel SCS also includes a standalone Discovery utility that you can use for this task instead of the Configurator. The utility contains only the `SystemDiscovery` command. The utility is located in the `SCS_Discovery` folder.<br>**Note:**<br>• On systems that do not have Intel AMT, this command gets data from the host platform only.<br>• For information about the data that is collected, refer to the `Intel(R)_SCS_Discovery.pdf`, located in the `SCS_Discovery` folder. |
| **Syntax** | `ACUConfig.exe [global options] SystemDiscovery {[<filename>] \| [/NoFile]} [/NoRegistry] [/AdminPassword <password>]` |
| **Parameters** | |

| | |
|---|---|
| `[global options]` | See CLI Global Options on page 83 |
| `<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. You can change this default name and location by supplying the `<filename>` parameter.<br>**Example:**<br>`ACUConfig.exe SystemDiscovery C:\MyXMLFile.xml`<br>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 83). |
| `/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 |
| `/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:<br>• The device is in an unconfigured state<br>• The user account running the Configurator is a Kerberos account that is configured in the Intel AMT device with administrator permissions |

# 5.7 Configuring Systems

| **Command** | `ConfigAMT` |
|---|---|
| **Description** | Configures Intel AMT with settings in a configuration profile (XML file). Configured systems are reconfigured. |
| **Syntax** | `ACUConfig.exe [global options] ConfigAMT <filename> [/DecryptionPassword <password>] [/AbortOnFailure] [/AdminPassword <password>] [/ADOU <ADOU path>] [/NetworkSettingsFile <file>] {[/FileToRun <filename>] [/FileHash <SHA256 hash>] [/FileUser <username>] [/FilePassword <password>]}` |
| **Parameters** | |
| `[global options]` | See CLI Global Options on page 83 |
| `<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 5) |
| `/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:<br>• The device is in an unconfigured state<br>• The XML profile contains the Digest admin password<br>• The user account running the Configurator is a Kerberos account that is configured in the Intel AMT device with administrator permissions |
| `/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 78. |
| `/FileToRun`<br>`/FileHash`<br>`/FileUser`<br>`/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 96. |

# 5.8 Configuring a System using a USB Key

| | |
|---|---|
| **Command** | `ConfigViaUSB` |
| **Description** | Creates a file containing configuration settings. When the Intel AMT system is rebooted with a USB key containing this file, Intel AMT is configured on the system. For more information, see SMB/Manual Configuration on page 4. The Configurator does not restrict the size of USB key you can use. But, the computer BIOS must fully support the selected USB key and be able to boot from it.<br>**Note:**<br>• The settings you can define are limited. If additional settings are required, they must be performed by a third-party application.<br>• This command puts the Intel AMT device in the Admin Control mode (see Control Modes on page 7).<br>• You can use this option to define certain KVM parameters not available in Client Control. |
| **Syntax** | `ACUConfig.exe [global options] ConfigViaUSB {/NewMEBxPass <password>} [/CurrentMEBxPass <password>] [/OutputFile <filename>] [/PowerPackage <guid>] {{/UsingDhcp}\| {/HostName <host_name> /DomainName <domain_name> /LocalHostIp <ip> /SubnetMaskIp <subnet_mask> [/GatewayAddrIp <ip> ] [/DnsAddrIp <ip>] [/SecondaryDnsAddrIp <ip>]}} [/EnableKVM <false \| true>] [/EnableUserConsent <none \| kvm_only \| all_redirection>] [/EnableRemoteITConsent <false \| true>]` |
| **Parameters** | |
| `[global options]` | See CLI Global Options on page 83 |
| `/NewMEBxPass <password>` | The new password to put in the Intel MEBX (see Password Format on page 5). This parameter is mandatory, even if the password has already been changed from the default of "admin". |
| `/CurrentMEBxPass <password>` | The current Intel MEBX password. The default password of unconfigured systems is "admin". This parameter is not required for systems that have the default password. |
| `/PowerPackage <guid>` | Power Package GUID (see Power Package GUIDs on page 89) |

| | |
|---|---|
| /OutputFile <filename> | The name of the file and the path to the location where you want to save it. If this parameter is not used, by default the file is created in the same folder as the Configurator. The file must be named Setup.bin and must be placed in the root folder of the USB key.<br>To make sure that Setup.bin is the first file that the BIOS will find during reboot (requirement), format the USB key before creating/copying the file. If the Intel AMT system does not successfully reboot with the USB key you prepared, try this:<br>• Make sure that the file name starts with a capital "S"<br>• Format the USB key using FAT16<br>**Note:**<br>• The Setup.bin file is NOT encrypted. Make sure that you restrict access to it.<br>• After configuration is complete, the Configurator deletes the data contained in the file. This means that you must create a new file for each system you want to configure.<br>• The Configurator overwrites any existing file with the same name without giving a warning. |
| /UsingDhcp | Sets the DHCP mode to enabled in the Intel MEBX |
| /HostName <host_name> | Intel AMT system hostname (1 – 32 characters) |
| /DomainName <domain_name> | Intel AMT system domain name (0 – 63 characters) |
| /LocalHostIp<ip> | The IP address (IPV4) to set in the Intel MEBX. If you supply this parameter, the /SubnetMaskIp parameter is mandatory (the remaining IP parameters are optional). |
| /SubnetMaskIp <subnet_mask> | The subnet mask IP address to set in the Intel MEBX |
| /GatewayAddrIp <ip> | The default gateway IP address to set in the Intel MEBX |
| /DnsAddrIp <ip> | The preferred DNS IP address to set in the Intel MEBX |
| /SecondaryDnsAddrIp <ip> | An alternate DNS IP address to set in the Intel MEBX |
| /EnableKVM <false \| true> | Enable/Disable support for KVM redirection.<br>**Note:** This parameter is mandatory on systems with Intel AMT 6.0 and higher. If you do not supply it, configuration will fail on those systems. |

| | |
|---|---|
| `/EnableUserConsent <none \| kvm_only \| all_redirection>` | Defines for which redirection operations user consent is mandatory.<br>For more information, see User Consent on page 8.<br>**Note:** You can use the `all_redirection` option only on systems with Intel AMT 7.x and higher. |
| `/EnableRemoteITConsent <false \| true>` | Defines if it is permitted to remotely make changes to the user consent setting in the Intel AMT device |

## 5.8.1 Power Package GUIDs

The optional `/PowerPackage` parameter enables you to define power management settings of the Intel AMT device during manual configuration. If not supplied, the default power settings defined by the manufacturer are used. This table gives the GUID values (in Hex 32 character format) per Intel AMT version.

| Supported Power Package | GUID (Hex 32) |
|---|---|
| **Intel AMT 6.x and higher (mobile)** | |
| ON in S0 | 763997110B56504388709812F391B560 |
| ON in S0, ME Wake in S3/AC, S4-5/AC | 30800DEE09C07843AF287868A2DBBE3A |
| **Intel AMT 6.x and higher (desktop)** | |
| ON in S0 | 944F8312FB104FDC968E1E232B0C9065 |
| ON in S0, ME Wake in S3,S4-5 | 7322734623DC432FA98A13D37982D855 |
| **Intel AMT 5.x (desktop)** | |
| ON in S0 | 944F8312FB104FDC968E1E232B0C9065 |
| ON in S0, S3 | A18600AB9A7F4C42A6E6BB243A295D9E |
| ON in S0, S3, S4-5 | 7286ABAC96B448E29B9E9B7DF91C7FD4 |
| ON in S0, ME WoL in S3 | 7B32CD4D6BBE4389A62A4D7BD8DBD026 |
| ON in S0, ME WoL in S3, S4-5 | 7322734623DC432FA98A13D37982D855 |
| ON in S0, S3, S4-5, OFF After Power Loss | C519A4BA6E6F8D4DB227517F7E4595DB |
| ON in S0, ME WoL in S3,S4-5, OFF After Power Loss | D60BE3ED04C52C46B772D18018EE2FC4 |
| **Intel AMT 4.x (mobile)** | |
| ON in S0 | 763997110B56504388709812F391B560 |
| ON in S0, S3/AC | 26D31C768708C74BBB5F38744315A5FF |
| ON in S0, S3/AC, S4-5/AC | 530E08DB6C0FD948B2D28958D3F1156E |

| Supported Power Package | GUID (Hex 32) |
|---|---|
| ON in S0, ME Wake in S3/AC | 055DD5B64CA4874DA5A8B47C14DEDA5F |
| ON in S0, ME Wake in S3/AC, S4-5/AC | 30800DEE09C07843AF287868A2DBBE3A |

# 5.9 Maintaining Configured Systems

| **Command** | `MaintainAMT` |
|---|---|
| **Description** | Runs specific maintenance tasks on Intel AMT, based on settings in the `<filename>` XML file. |
| **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 83 |
| `<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:<br>• `SyncAMTTime` – Synchronizes the clock of the Intel AMT device with the clock of the host. This task is performed automatically when any of the other tasks are performed.<br>• `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 78)<br>• `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.<br>• `RenewADPassword` – Changes the password of the Active Directory object representing the Intel AMT system.<br>• `RenewAdminPassword` – Changes the password of the default Digest admin user in the Intel AMT device according to the password setting defined in the profile.<br>• `AutoMaintain` – Automatically does only the maintenance tasks (listed here) that are necessary for this Intel AMT system.<br>For more information, see:<br>• About Maintenance Tasks on page 12<br>• Manual/Automatic Maintenance using the CLI on page 14 |
| `/DecryptionPassword <password>` | Mandatory if any of the files that the Configurator will use are encrypted (see File Encryption on page 5) |
| `/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:<br>• The XML profile contains the Digest admin password<br>• The user account running the Configurator is a Kerberos account that is configured in the Intel AMT device with administrator permissions |
| `/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 78. |
| `/FileToRun`<br>`/FileHash`<br>`/FileUser`<br>`/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 96. |

# 5.10 Unconfiguring Intel AMT Systems

| | |
|---|---|
| **Command** | `Unconfigure` |
| **Description** | Unconfigures Intel AMT. There are two types of unconfiguration:<br>• **Partial** – Removes the configuration settings from the system and disables the Intel AMT features on the system. (The PID, PPS, admin ACL settings, host name, and domain name 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.<br>• **Full** – Deletes all the Intel AMT settings from the system and disables the Intel AMT features on the system.<br>**Note:**<br>• Systems in Client Control mode are always unconfigured with a "Full" unconfiguration.<br>• The default unconfiguration type for systems in Admin Control mode is "Partial". |
| **Syntax** | `ACUConfig.exe [global options] UnConfigure [/AdminPassword <password>] [/Full] [/ADOU <ADOU path>] {[/DomainUser <username>] [/DomainUserPassword <password>]} [/SourceForAMTName <source>] [/NetworkSettingsFile <file>]` |
| **Parameters** | |
| [global options] | See CLI Global Options on page 83 |
| `/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:<br>• The XML profile contains the Digest admin password<br>• The user account running the Configurator is a Kerberos account that is configured in the Intel AMT device with administrator permissions |

| | |
|---|---|
| /Full | For systems in Admin Control mode, does a full unconfiguration (the default is partial unconfiguration). Full unconfiguration also deletes customized data. For example:<br>• Any root certificate hashes that were entered manually into the Intel MEBX<br>• Any customized data that was pre-defined by the manufacturer (for example, the PKI DNS Suffix)<br>**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.<br>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. By default, the credentials of the user running the Configurator are used to delete the AD object. If you supply this parameter, the AD object is deleted using the credentials of this user. |
| /DomainUserPassword <password> | The password of the domain user |

| | |
|---|---|
| /SourceForAMTName <source> | Defines how the FQDN (hostname.suffix) for the Intel AMT device is constructed. Valid values:<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>• HOST — Takes the hostname from the host operating system. The suffix is blank.<br>**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. |

# 5.11 Running Scripts with the Configurator

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 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.

For more information, see:


- Scripts Run by the Configurator on the next page
- What if a Failure Occurs? on page 97
- Script Runtime and Timeout on page 98
- Parameters Sent in Base64 Format on page 98

## 5.11.1 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 5-1: 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 6). 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. |
| 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.<br>For example: `SHA256.exe MyFile.bat`<br>will return the hash value of `MyFile.bat`.<br>The hash value is marked in blue. Copy the value and supply it in the `<SHA256 hash>` parameter. |
| `/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 5-2: 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.) | |

## 5.11.2 What if a Failure Occurs?

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 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.

## 5.11.3 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"

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.

## 5.11.4 Parameters Sent in Base64 Format

Some of the parameters sent by the Configurator 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.

# 5.12 Configurator Return Codes

This table describes the return codes that are shown and recorded in the log file when running Configurator CLI commands. (For informational purposes, the list includes all return codes. Return codes related to remote configuration and the RCS should never occur when not using the RCS.)

Table 5-3: Configurator Return Codes

| # | Description |
|---|---|
| 0 | The requested operation completed successfully |
| 1 | Intel AMT is already configured on this system |
| 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) |
| 18 | Cannot write the USB configuration data to file (possible reasons- the specified path does not exist; no write permissions; not enough free space). |
| 19 | Failed to create the USB configuration file (invalid IP) |
| 20 | Failed to create the USB configuration file (invalid power package) |
| 21 | An internal error occurred when creating the USB configuration file |
| 22 | An internal exception occurred when processing the request |

| # | Description |
|---|---|
| 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 |
| 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) |
| 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 |
| 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 |

| # | Description |
|---|---|
| 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 |
| 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 |

| # | Description |
|---|---|
| 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. |
| 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 |

| # | Description |
|---|---|
| 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. |

# Chapter 6

## Preparing the Certification Authority

This chapter describes the prerequisites and procedures for using a Certification Authority (CA) with Intel SCS.

For more information, see:


6.1 About Certification Authorities ..... 105
6.2 Using Intel SCS with a Microsoft CA ..... 105
6.3 Using Predefined Files Instead of a CA Request ..... 113
6.4 Defining Common Names in the Certificate ..... 114
6.5 CRL XML Format ..... 116

# 6.1 About Certification Authorities

A 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.
- Using predefined files

# 6.2 Using Intel SCS with a Microsoft CA

This section describes the prerequisites necessary to use Intel SCS with a Microsoft CA.

## 6.2.1 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. 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

## 6.2.2 Required Permissions on the CA

These permissions are required on the CA by the user account running Intel SCS component doing the configuration:

- Issue and Manage Certificates
- Request Certificates

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.

## 6.2.3 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 (shown in yellow in this figure).

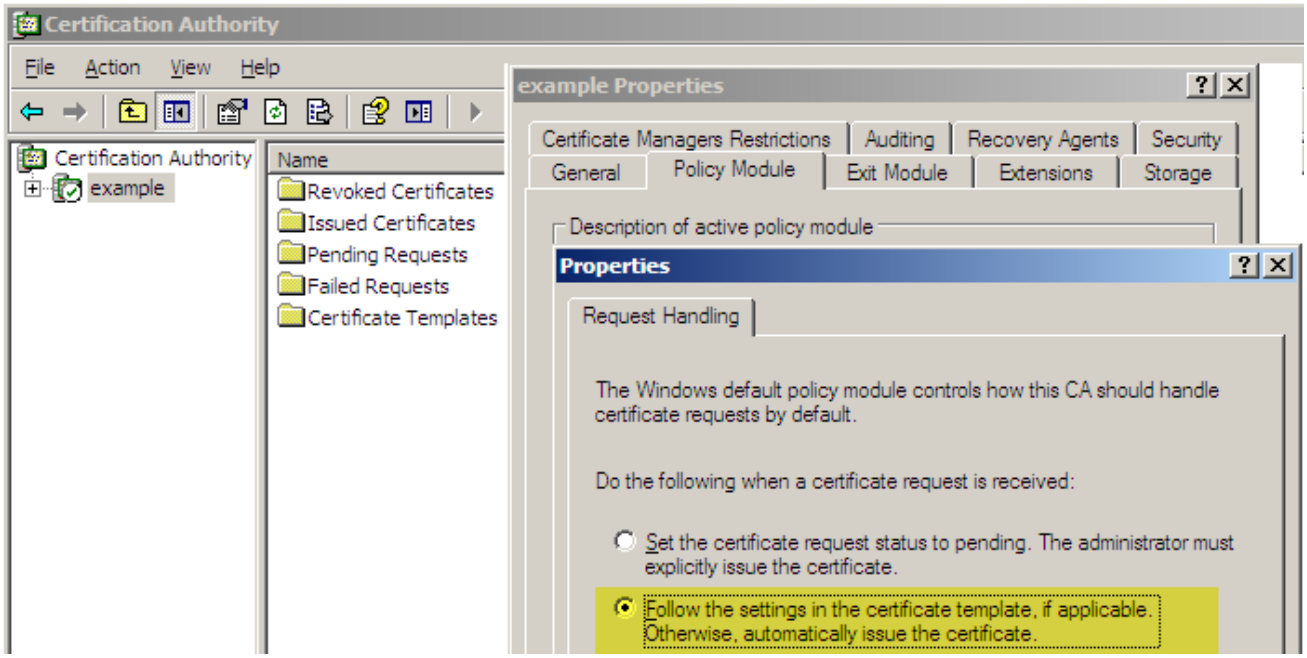



Figure 6-1: Request Handling Tab

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 (shown in yellow in this figure).

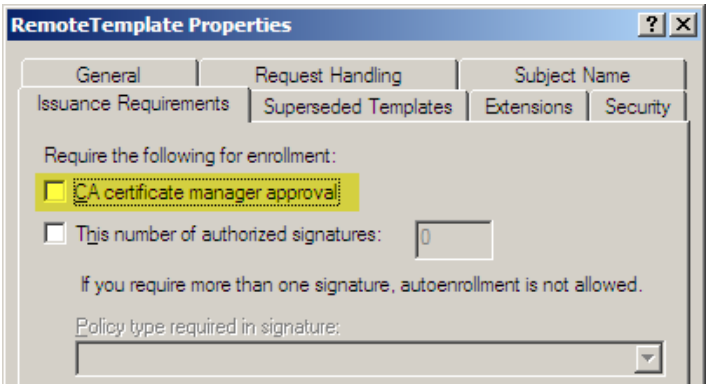



Figure 6-2: Issuance Requirements Tab

## 6.2.4 Defining Enterprise CA Templates

If you use Intel SCS with an Enterprise CA to 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 the previous page.

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

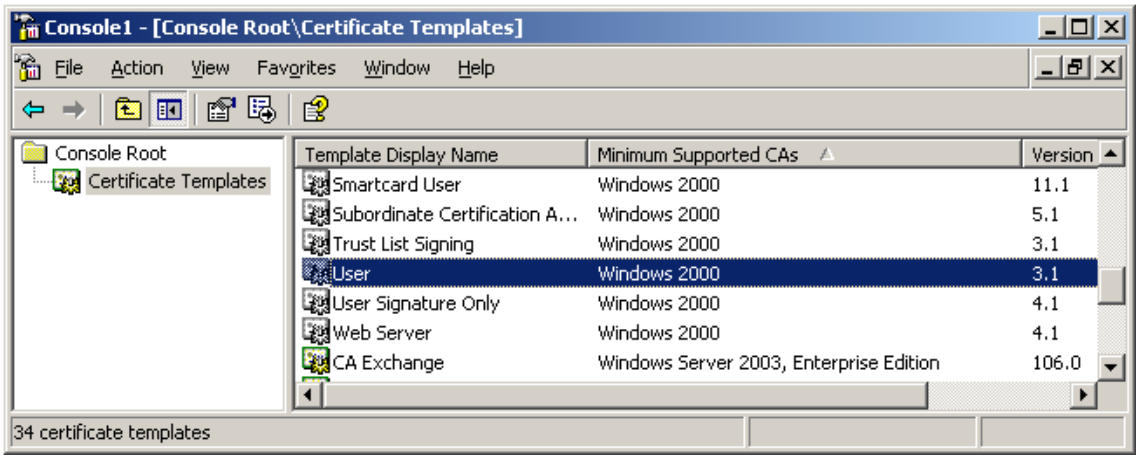



Figure 6-3: Microsoft Management Console

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

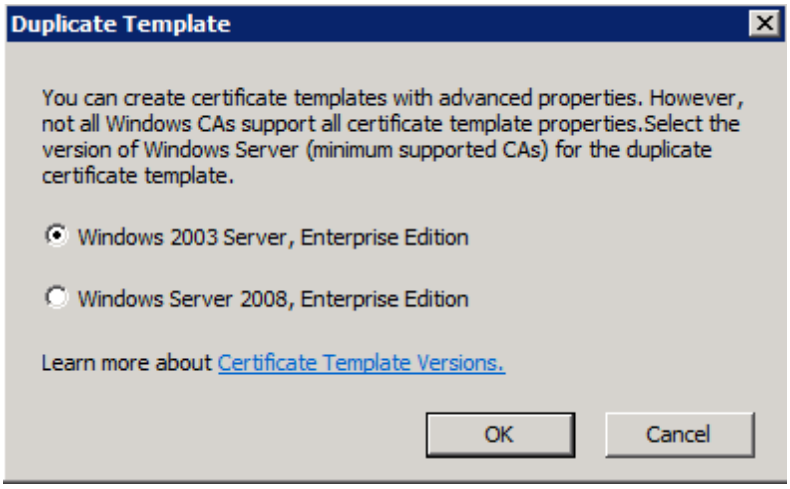



Figure 6-4: Duplicate Template Window

> **Note:**
>
> Intel SCS supports only version 2 certificate templates. Version 3 certificate templates are not supported and cannot be selected in the configuration profile (they will not be shown in the list).

6. Make sure that you select **Windows Server 2003 Enterprise**.

7. Click **OK**. The Properties of New Template window opens.

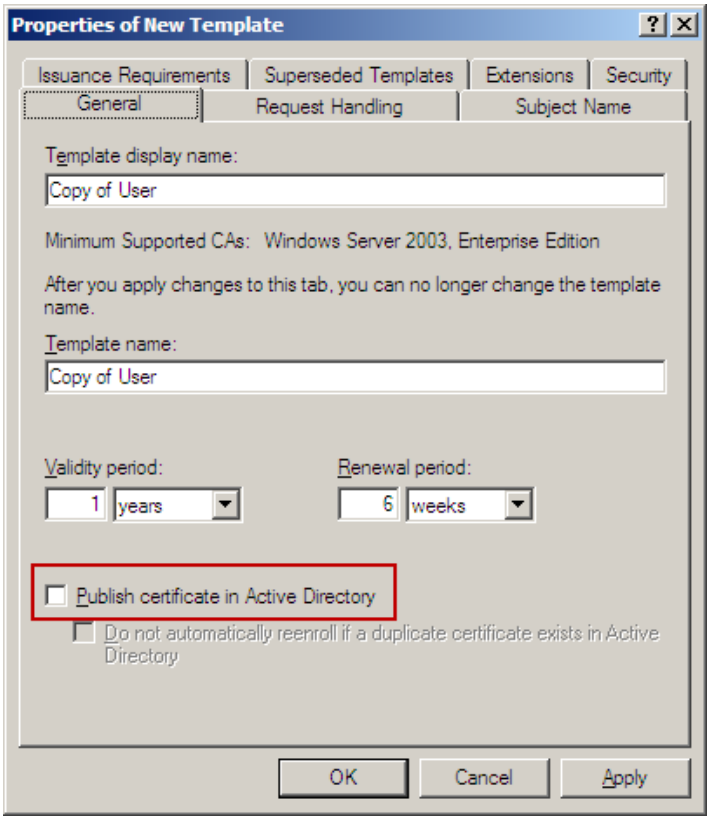



Figure 6-5: Properties of New Template Window

8. Make sure that the **Publish certificate in Active Directory** check box is NOT selected.
9. In the Template display name field, enter a meaningful name. For example, name a template used to generate 802.1x client certificates "802.1x".
10. Change the validity and renewal periods as required by local policy and click **Apply**.

11. Click the **Request Handling** tab. The Request Handling tab opens.

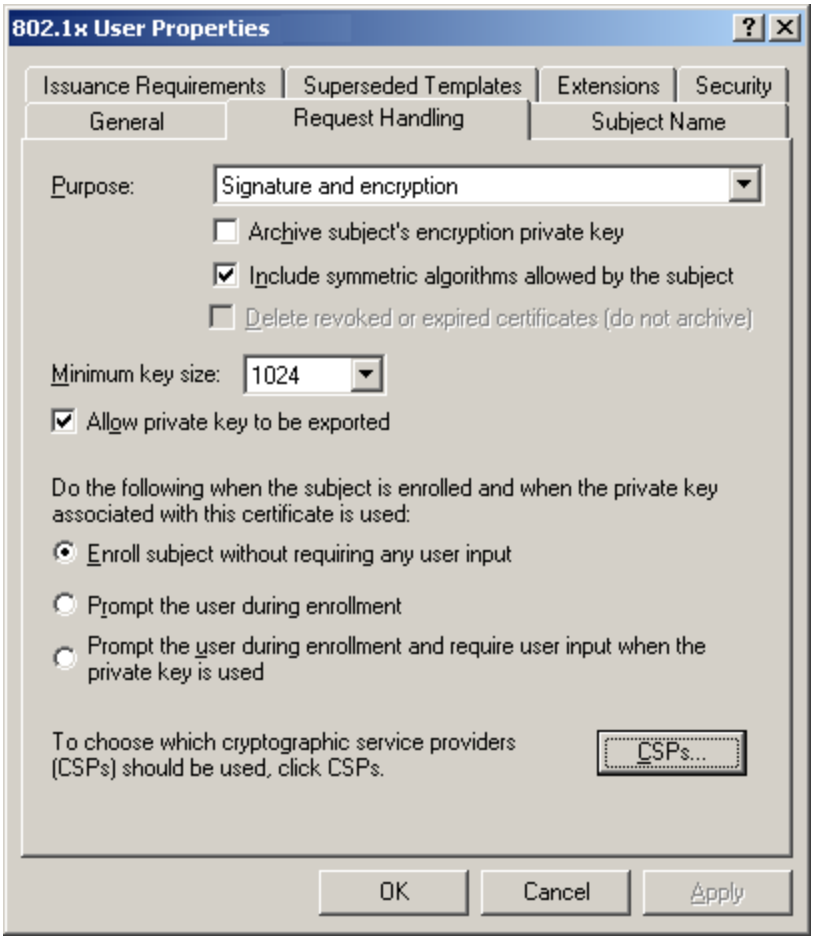



Figure 6-6: Request Handling Tab

**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.

12. Click the **CSPs** button. The CSP Selection window opens.

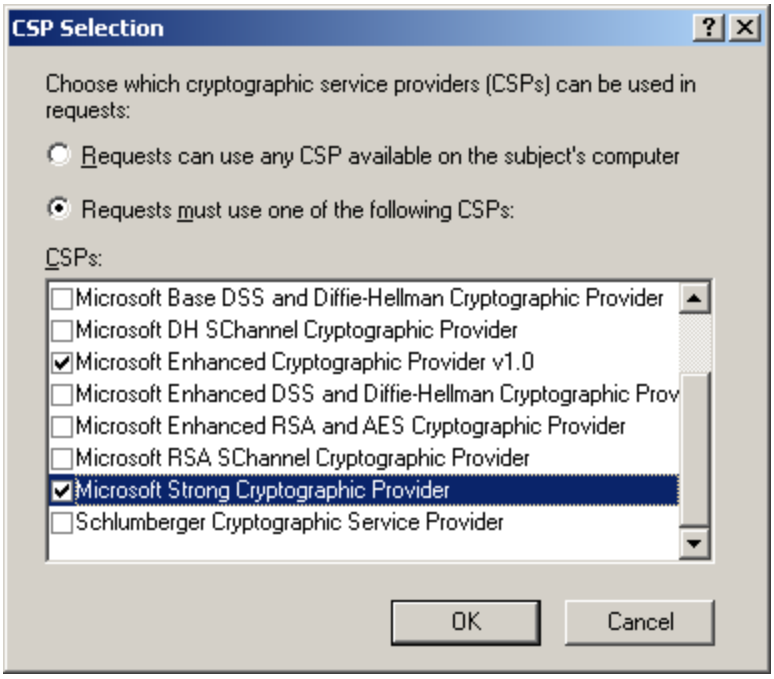



Figure 6-7: CSP Selection Window

13. In the list of requests, select the **Microsoft Strong Cryptographic Provider** check box and click **OK**. The CSP Selection window closes.
14. Click the **Subject Name** tab and select **Supply in the request**.
15. Click the **Security** tab. The Security tab opens.
16. 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.

17. If this is a template for TLS, do these steps:

    a. Click the **Extensions** tab. The Extensions tab opens.

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

    c. Click **Add**. The Add Application Policy window opens.

    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.

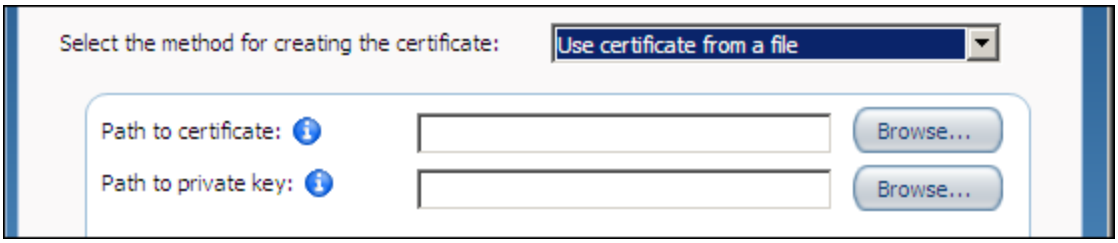
18. Click **OK**. The Properties of New Template window closes.
19. Select **Start** > **Programs** > **Administrative Tools** > **Certification Authority**.
20. From the Console Root tree, select **Certificate Authority** > **Certificate Templates**.
21. Right-click in the right pane and select **New** > **Certificate Template to Issue**. The Enable Certificate Templates window opens.
22. Select the template that you just created and click **OK**. The Enable Certificate Templates window closes and the template is added to the right pane with the other certificate templates.
23. Restart the CA (to publish the new template in the Active Directory).

# 6.3 Using Predefined Files Instead of a CA Request

Usually, during configuration of Intel AMT features defined to use certificate-based authentication, Intel SCS requests the certificate from a CA. To do this, Intel SCS must have access to the CA during configuration. However, in some network environments the CA cannot be accessed from all computers.

The host-based configuration method supplies a solution to this problem. When defining certificate-based authentication, you can now use predefined certificates and private key files (used for the encryption).

To do this, select the **Use certificate from a file**, option:




**Note:**

For each file you can click **Browse** to locate and select it, or enter the path to it from the Intel AMT system. However, make sure that you put both files in a location that can be accessed from the Intel AMT system. Two such files are required per Intel AMT system.

## Required Format for Certificate and Key Files

The files that you supply must be in the Base64 format, known as the PEM format. The information in each file must be enclosed between a correct "BEGIN" header line (starting with five dashes) and an "END" footer line.

**For certificate files:**

-----BEGIN CERTIFICATE-----

... (CA certificate in bases encoding) ...

-----END CERTIFICATE-----

**For key files you must use only the "PKCS#1 RSAPrivateKey" format:**

-----BEGIN RSA PRIVATE KEY-----

...(Key in RSA PKCS#1 format)...

-----END RSA PRIVATE KEY-----

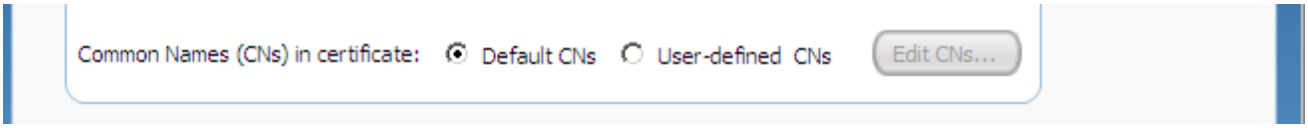
**Note:**

If necessary for your network environment, you can encrypt the private key file (see File Encryption on page 5).

# 6.4 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).

> **Note:**
>
> These fields are not shown if you select the "Use certificate from file" option.

## 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.

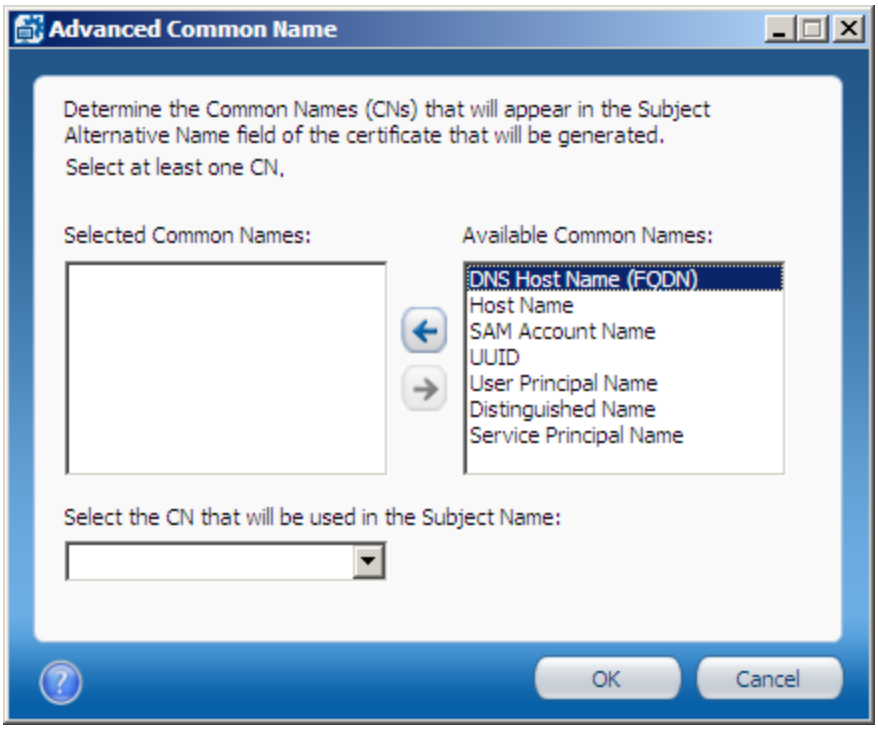



Figure 6-8: Advanced Common Name Window

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.

# 6.5 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 64).

**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="15278220000000000003"/>
</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 7

## Troubleshooting

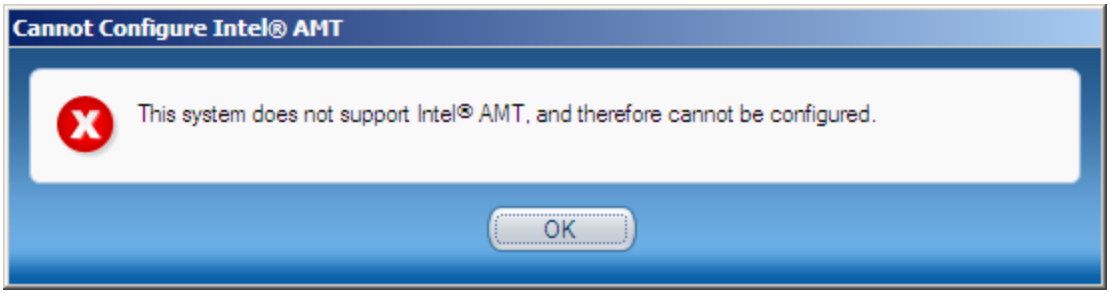
This chapter describes problems you might find when using Intel SCS, and provides their solutions.

For more information, see:


7.1 Configuration Utility Error: "Cannot Configure Intel AMT" ..... 118
7.2 The Configuration Utility Takes a Long Time to Start ..... 118
7.3 Problems Using Configuration Utility on a Network Drive ..... 119
7.4 Exit Code 88 ..... 120
7.5 Exit Code 110 ..... 120
7.6 Remote Connection to Intel AMT Fails ..... 121
7.7 Error with XML File or Missing SCSVersion Tag ..... 122
7.8 Reconfiguration of Dedicated IP and FQDN Settings ..... 122
7.9 Disjointed Namespaces ..... 123
7.10 Kerberos Authentication Failure ..... 124
7.11 Error: "Kerberos User is not Permitted to Configure.." ..... 124
7.12 Error: "The Caller is Unauthorized." ..... 124
7.13 Error when Removing AD Integration (Error in SetKerberos) ..... 125
7.14 Failed Certificate Requests via Microsoft CA ..... 125
7.15 Delta Profile Fails to Configure WiFi Settings ..... 126
7.16 Disabling the Wireless Interface ..... 126

# 7.1 Configuration Utility Error: “Cannot Configure Intel AMT”

The Welcome window of the Configuration Utility includes an option named “Configure/Unconfigure this System”. If you select this option when the Configuration Utility is running on a system that does not have Intel AMT, this error message shows:




This is because you can use this option only when you run the Configuration Utility on systems that have Intel AMT.

But, in this version of the Configuration Utility, this error message can also occur for systems that have Intel AMT. This is a known issue and only occurs on Intel AMT 5.x or lower when Intel AMT is disabled in the MEBX.

**Solution:**

Enable Intel AMT in the Intel MEBX.

# 7.2 The Configuration Utility Takes a Long Time to Start

To use the Configuration Utility, Microsoft .NET Framework must be installed on the computer. Some versions of the .NET Framework include limitations that can cause the Configuration Utility to take a long time to start. To prevent these problems, the ACUWizard.exe.config file includes this setting:

<runtime>

<generatePublisherEvidence enabled="false"/>

</runtime>

However, not all versions of .NET support this setting.

**Solution:**

Make sure that the version of .NET Framework installed on the computer supports the generatePublisherEvidence setting.

For example: Version 2.0 (service pack 1) or version 3.0 (service pack 1).

## 7.3 Problems Using Configuration Utility on a Network Drive

Due to security measures built into .NET Framework, if you try to start the Configuration Utility on a network drive, you might receive this error message:

"Intel® Active Management Technology Configuration Utility has encountered a problem and needs to close."

**Solution:**

Give "Full Trust" to the network share as shown in this example:

cd c:\WINDOWS\Microsoft.NET\Framework\v2.0.50727

CasPol.exe -m -ag 1.2 -url file:///N:/your/network/path/* FullTrust

## 7.4 Exit Code 88

This error means that authentication of the ACU.dll file (used by the Configurator) has failed and the requested operation was aborted. This error means that the file is corrupted and thus is not trusted by Intel SCS. Reasons for corruption can include changes made to the file by viruses or hardware failures.

## 7.5 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

# 7.6 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, your management console will not be able to connect to the device.

**Solutions:**

The first step is to check the IP address that is defined in the Intel AMT device. To do this, use the standalone Discovery Utility or the `SystemDiscovery` command. For more information, see Discovering Systems on page 84.

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.

## 7.7 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:**

- 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 Intel SCS 10.0. (Profiles created using Intel SCS 7.1 include this tag and are valid for use by Intel SCS 10.0.)

  **Note:**

  Try and open the profile using the Intel AMT Configurator Utility supplied in Intel SCS 10.0. 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 and Windows Server 2008. This is because of a known Microsoft issue. Install this hotfix: http://support.microsoft.com/kb/981118.

## 7.8 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.

# 7.9 Disjointed Namespaces

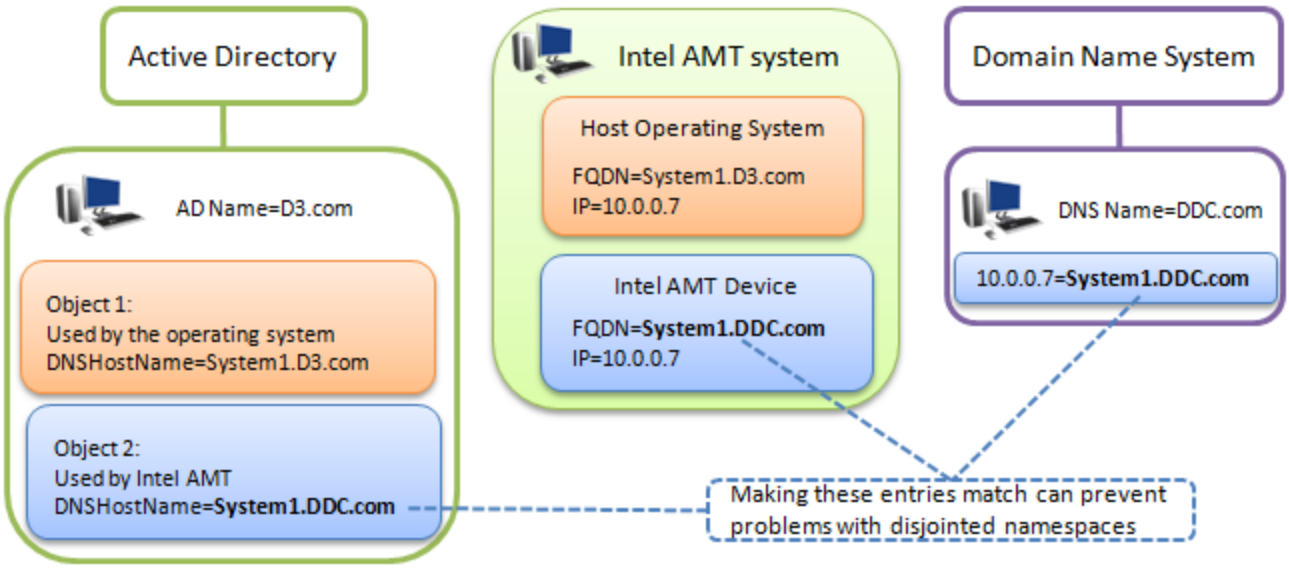
A disjointed namespace occurs when the primary Domain Name System (DNS) suffix of a computer does not match the DNS domain of which it is a member. Defining a network environment with disjointed namespaces (intentionally or accidentally) can cause many different types of communication and authentication 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 78).

## 7.10 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 49). 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.)

## 7.11 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.

## 7.12 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.

## 7.13 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.

## 7.14 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 114).

## 7.15 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 10. (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.

## 7.16 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 48).

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.