Intel® Setup and Configuration Software (Intel® SCS)
Deployment Guide

Version 1.0

Document Release: August 2015
Table of Contents

1 Introduction .................................................................................................................. 7
  1.1 Intel® Setup and Configuration Software (Intel® SCS) Overview ...................... 8
  1.2 Intel® Active Management Technology (Intel® AMT) Overview ...................... 9

2 Prerequisites .................................................................................................................. 10
  2.1 Client Software Components .............................................................................. 10
  2.2 Supported Operating Systems ......................................................................... 11
  2.3 Supported Microsoft SQL Server Versions ...................................................... 11
  2.4 Network Access and Network Ports ................................................................. 12
  2.5 Domain Name System (DNS) .......................................................................... 12
  2.6 Dynamic Host Configuration Protocol (DHCP) ................................................ 12
  2.7 Microsoft Certificate Authority (CA) ............................................................... 13
  2.8 Microsoft Active Directory (AD) ...................................................................... 13

3 Discovery ....................................................................................................................... 14
  3.1 Introduction ......................................................................................................... 14
  3.2 Using the Configurator ..................................................................................... 14
  3.3 Using the SCS_Discovery Utility ..................................................................... 16
  3.4 Using the RCS ................................................................................................... 17
  3.5 Using the Platform Discovery Utility ................................................................. 17
  3.6 Using the Solutions Framework ....................................................................... 17

4 Configuration ................................................................................................................ 18
  4.1 Introduction ......................................................................................................... 18
  4.2 Configuration Methods ..................................................................................... 18
  4.3 Host-Based Configuration .................................................................................. 19
  4.4 Using the Intel AMT Configuration Utility Wizard ........................................... 19
  4.5 Using the Intel AMT Configuration Utility Command Line Interface (CLI) .... 22
  4.6 Manual Configuration ....................................................................................... 23
  4.7 Manual Configuration (Multiple Systems) ......................................................... 25
  4.8 Remote Configuration Using PKI ...................................................................... 26
  4.9 Unconfigure Method ......................................................................................... 26

5 Install and Configure Intel RCS and Console ......................................................... 29

6 Intel AMT Provisioning Certificates ......................................................................... 34
  6.1 Introduction ......................................................................................................... 34
  6.2 Prerequisites ....................................................................................................... 36
  6.3 Reference ............................................................................................................. 36
  6.4 Generate Certificate Signing Request (CSR) .................................................... 38
  6.5 Submit Certificate Signing Request (CSR) ......................................................... 38
  6.6 Merge Issued Certificate .................................................................................... 39
  6.7 Installing Root and Intermediate Certificates .................................................... 39
  6.8 Install and Validate the Certificate .................................................................... 40
6.9 Verify and Validate Remote Configuration Using PKI ........................................... 43
6.9.1 Create AMT Profile .................................................................................. 43
6.9.2 Apply AMT Profile .................................................................................. 44
6.10 Verify AMT Connectivity ........................................................................... 44

7 Microsoft Active Directory ............................................................................. 46
7.1 Introduction ................................................................................................. 46
7.2 Prerequisites ............................................................................................... 47
  7.2.1 Create New OU ....................................................................................... 47
  7.2.2 Create New AD Groups ......................................................................... 47
  7.2.3 Create New Local Groups ....................................................................... 48
  7.2.4 Assign Permissions to New OU ............................................................... 49
7.3 Verify and Validate Microsoft Directory Integration ................................... 49
  7.3.1 Create AMT Profile ................................................................................ 49
  7.3.2 Apply AMT Profile ................................................................................ 51
  7.3.3 Verify AMT Connectivity ....................................................................... 51

8 Secure Communications Using Transport Layer Security (TLS) ..................... 52
8.1 Introduction .................................................................................................. 52
8.2 Prerequisites ............................................................................................... 52
  8.2.1 Request Handling .................................................................................. 53
  8.2.2 Create Certificate Template .................................................................. 53
  8.2.3 Configure Certificate Template ............................................................... 54
  8.2.4 Assign Permissions to Certificate Template .......................................... 56
  8.2.5 Issue Certificate Template .................................................................... 57
8.3 Verify and Validate Transport Layer Security (TLS) Configuration ............. 59
  8.3.1 Create AMT Profile ................................................................................ 59
  8.3.2 Apply AMT Profile ................................................................................ 60
  8.3.3 Verify AMT Connectivity ....................................................................... 60

9 Wireless .......................................................................................................... 62
9.1 Introduction .................................................................................................. 62
9.2 Prerequisites ............................................................................................... 62
  9.2.1 PKI DNS Suffix ...................................................................................... 63
9.3 Discover ....................................................................................................... 64
9.4 Remotely Configuring LAN-less Systems .................................................... 65
  9.4.1 Create AMT Profile ................................................................................ 65
  9.4.2 Apply AMT Profile (Host-Based Configuration) ...................................... 66
  9.4.3 Move system to Admin Control mode ................................................... 67
1 Introduction

This deployment guide is an instructional document providing simple steps to enable the discovery, configuration and integration of Intel® Active Management Technology (Intel® AMT) platforms using Intel® Setup and Configuration Software (Intel® SCS).

Intel AMT operates independently of the CPU and the firmware is delivered in an un-configured state. Intel SCS is provided by Intel to support the setup and configuration of the firmware for the target environment and enable remote, out-of-band access to Intel AMT features.

Guidance is provided to enable a baseline implementation of Intel AMT and identifies common configuration settings to support an enterprise deployment that takes advantage of the manageability and security features available on platforms that support Intel® vPro™ Processor technology and Intel® Standard Manageability 1

After configuration, Intel AMT systems can be remotely managed by products, toolsets and solutions including McAfee ePO Deep Command*, Microsoft System Center Configuration Manager*, Microsoft PowerShell*, VNC® Viewer Plus.

Examples of where Intel AMT delivers value to IT and the business include:

- Utilize hardware based Remote Control to reduce maintenance and support costs and avoid desk-side visits.
- Improving system deployment and rebuild processes.
- Keep clients securely updated and avoid working hours reboots, even for remote employees.
- Providing effective remote assistance whilst outside the corporate network.
- Providing a secure and effective decommission process for retired machines.


---

1 Intel® Standard Manageability (ISM) systems were introduced with Intel AMT Release 5.0 and have a subset of Intel AMT features i.e. no KVM, Alarm Clock, WLAN etc.

* Other names and brands may be claimed as the property of others.
1.1 Intel® Setup and Configuration Software (Intel® SCS) Overview

Intel® Setup and Configuration Software (Intel® SCS) is a collection of software components and utilities developed by Intel and used to discover, configure and maintain Intel® Active Management Technology (Intel® AMT) platforms within your network. Intel SCS benefits include:

- Free, supported product that enables a consistent and standard approach to the setup and configuration of Intel AMT manageability and security features available on Intel® vPro™ Processor technology and Intel® Standard Manageability platforms.
- Robust enterprise features including support for the latest releases of Microsoft Operating Systems and SQL Server and proven scalability to discover, configure and maintain 10’s of thousands of Intel AMT systems.
- Rich Software Development Kit (SDK) provides future-proof stability for developers and support for third party solutions.

Intel SCS includes the following components, however only some of these are used or referenced within this guide. Please reference the Intel® Setup and Configuration Software (Intel® SCS) User Guide (Intel(R) _SCS_User_Guide.pdf), for additional details:

- **Remote Configuration Service (RCS):** A Windows* based service that runs on a physical computer or VM within your network. The RCS processes configuration requests and can handle the storage of data.
- **Console:** This is the user interface to the RCS and is used to create and edit configuration profiles. In database mode, the Console allows you to view data sent to the RCS and additional options including monitoring and performing maintenance tasks against multiple Intel AMT systems.
- **Configurator:** ACUConfig.exe is a Command Line Interface (CLI) used to configure Intel AMT (only) and runs locally on each Intel AMT system.
- **Intel AMT Configuration Utility:** ACUWizard.exe provides a GUI based wizard to quickly configure individual Intel AMT systems or create XML profiles.
- **Discovery Utility:** This is a standalone utility used to gather detailed information about Intel AMT.
- **Remote Configuration Service Utility:** RCSUtil.exe is a Command Line Interface (CLI) used to make some of the RCS setup tasks easier including installing certificates and assigning Windows Management Instrumentation (WMI) permissions to user accounts.
- **Solutions Framework:** Extends the capability of Intel SCS to discover and configure other Intel products in addition to Intel AMT.
- **Database Tool:** Used to perform some of the tasks necessary when installing the RCS in database mode i.e. Intel SCS database creation.
- **Encryption Utility:** Used to encrypt and decrypt XML files used by Intel SCS.
1.2 Intel® Active Management Technology (Intel® AMT) Overview

Intel AMT is a component of the Intel® Management Engine (Intel® ME) and provides out-of-band (OOB) management within the physical chipset of Intel® vPro™ Processor technology and Intel® Standard Manageability platforms. Once the Intel AMT firmware has been configured using Intel SCS components, computers can be remotely accessed when they are powered off or the operating system is unavailable. The only requirements are that the system is connected to a power supply and has a wired (LAN) and/or wireless (WLAN) network connection.

When using the wired LAN interface on a corporate network, Intel AMT traffic shares the same physical network interface as the host operating system. Network traffic (on ports 16992-16995) is directly intercepted by Intel AMT before being passed to the host operating system. Network traffic received on an Intel AMT enabled wireless interface goes to the host wireless driver which detects the destination port and sends the message to Intel AMT.

A configured Intel AMT environment contains hardware, firmware and software that controls AMT features and capabilities. These components include:

- The Intel® Management Engine (Intel® ME) firmware.
- The Intel® Management Engine BIOS Extension (Intel® MEBX) is a BIOS menu extension on the Intel AMT system that can be used to view and manually configure some of Intel AMT settings. The menu is only displayed if you press a special key combination (traditionally <Ctrl-P> during the system BIOS boot process).
- The Intel® Management Engine Interface2 (Intel® MEI) driver, is the operating software interface to the Intel AMT device.
- The Intel® Local Manageability Service3 4 (LMS.exe) provides OS-related Intel(R) ME functionality.
- The Intel Management and Security Status (IMSS) provides status information to the local user about Intel AMT including messages and an indication that Intel AMT is configured.

---

2 MEI and LMS installed by the OEM. If they're missing or need to be reinstalled, check the OEM's support site to locate the correct versions for your system.
3 The LMS is installed on a platform that has Intel AMT Release 9.0 or greater.
4 From Intel AMT Release 2.5 to 8.1, LMS functions were performed by the User Notification Service (UNS).
2 Prerequisites

This section identifies the main requirements for enabling Intel AMT. For additional detail please reference the Intel Setup and Configuration Software (Intel SCS) User Guide, available in the Intel SCS download package.

NOTE: Dependent upon the configuration path chosen, you may not need to install the Intel SCS components, RCS and Console or a database.

2.1 Client Software Components

The Intel Management Engine software is a requirement on all Intel AMT systems. This is either pre-installed or available via the OEM's support site and consists of the following components:

- The Management Engine Interface (MEI) driver provides the software interface to the Intel AMT device and is installed as a system device.
- The Intel Local Manageability Service (LMS.exe) is a Windows service installed on an Intel AMT system that has Intel AMT Release 9.0 or greater. LMS enables local applications to send requests and receive responses to and from the Intel Management Engine, via the Intel MEI.
- From Intel AMT Release 2.5 to 8.1, LMS functions were performed by the User Notification Service (UNS).
- The Intel Management and Security Status (IMSS) provides status information to the local user about Intel AMT including messages and an indication that Intel AMT is configured.
- Serial-Over-LAN (SOL) device installed as a COM port.

NOTE: The Intel Management Engine software has a separate version for every Intel AMT generation (6.x, 7.x, 8.x, 9.x etc.). The Management Engine 10.x software also supports 9.x and 8.x generations.
2.2 Supported Operating Systems

The following table describes which operating systems the main Intel SCS components can run on.

<table>
<thead>
<tr>
<th>Version</th>
<th>Configurator</th>
<th>RCS</th>
<th>Console</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows® 8.1 Pro</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Windows 8.1 Enterprise</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Windows 8 Pro</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Windows 8 Enterprise</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Windows 7 Professional (SP1)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows 7 Enterprise (SP1)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows XP Professional (SP3)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Windows Server® 2012 R2</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Server 2008 R2 (SP2)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Server 2008 (SP2)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

2.3 Supported Microsoft SQL Server Versions

When the RCS is configured to support database mode, Intel SCS 10 now supports the Standard and Enterprise editions of Microsoft SQL Server 2012 and 2014 (marked in yellow).

<table>
<thead>
<tr>
<th>Version</th>
<th>Enterprise</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server 2014</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft SQL Server 2012</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft SQL Server 2008 R2 (SP1 and higher)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Microsoft SQL Server 2008 (SP1 and higher)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Microsoft SQL Server 2005 (SP4)</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
2.4 Network Access and Network Ports

Intel AMT supports two types of network access; local and remote. Intel AMT Releases 2.5, 2.6, 4.0, 6.0 and later support a wireless and wired network interface (remote) and a local interface (local applications running on the platform).

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>16992</td>
<td>Intel(R) AMT HTTP</td>
<td>Used for WS-Management messages to and from Intel AMT. The port is always open locally and only open over the network only when Intel AMT is configured or during the configuration process.</td>
</tr>
<tr>
<td>16993</td>
<td>Intel(R) AMT HTTPS</td>
<td>Used for WS-Management messages to and from Intel AMT when TLS is enabled.</td>
</tr>
<tr>
<td>16994</td>
<td>Intel(R) AMT Redirection/TCP</td>
<td>Used for redirection traffic (SOL, IDER, and KVM using Intel AMT authentication).</td>
</tr>
<tr>
<td>16995</td>
<td>Intel(R) AMT Redirection/TLS</td>
<td>Used for redirection traffic (SOL, IDER, and KVM using Intel AMT authentication) when TLS is enabled.</td>
</tr>
<tr>
<td>623</td>
<td>ASF Remote Management and Control Protocol (ASF-RMCP)</td>
<td>Used for RMCP pings. This port is a standard DMTF port and accepts WS-Management traffic. It is always enabled.</td>
</tr>
<tr>
<td>664</td>
<td>DMTF out-of-band secure web services management protocol</td>
<td>Used for secure RMCP pings. This port is always enabled and is a standard DMTF port that accepts secure WS-Management traffic.</td>
</tr>
<tr>
<td>5900</td>
<td>VNC (Virtual Network Computing) - remote control program</td>
<td>Used for KVM viewers that do not use Intel AMT authentication but use the standard VNC port instead.</td>
</tr>
</tbody>
</table>

**Note:** Dependent upon the configuration path chosen, the following infrastructure components may or may not be required.

2.5 Domain Name System (DNS)

Intel SCS configures the FQDN of the Intel AMT system which this is one of the most important configuration settings as these are shared with the host platform. As such DNS is highly recommended for IP resolution. The hostname is from the host operating system, whilst the suffix is the “Primary DNS Suffix” provided by DHCP Option 15.

2.6 Dynamic Host Configuration Protocol (DHCP)

On an Intel AMT system, the host platform and the Intel AMT device both have an IP address which are usually the same, however these can be different. Intel SCS components will configure the IP address of the Intel AMT device and by
default configures the Intel AMT device to get the IP address from a DHCP server. IPv4 addresses are supported, with IPv6 being supported from Intel AMT Release 6.0.

2.7 **Microsoft Certificate Authority (CA)**

A Certification Authority (CA) is a prerequisite for configuring **Secure Communications Using Transport Layer Security (TLS)** and certain Intel AMT features including Transport Layer Security (TLS), Remote Access, 802.1x and End-Point Access Control. The last three capabilities will require an Enterprise CA. However within the scope of this guide and when configuring TLS, this can performed by an Enterprise CA or a Standalone CA.

2.8 **Microsoft Active Directory (AD)**

Intel AMT can be optionally configured to integrate with Microsoft Active Directory this is recommended for enterprise environments that require Kerberos authentication of Microsoft Windows domain users or groups when interacting with Intel AMT.
3 Discovery

3.1 Introduction

Discovery provides detailed information on current configuration states, specific firmware versions, features and capabilities for Intel AMT platforms systems within your environment and helps determine the most appropriate configuration approach. Using Intel SCS utilities, data can be gathered about Intel AMT and the host platform and saved to an XML file on the system and/or written to the registry. Alternatively an option exists to send this data to the Remote Configuration Service (RCS) and save it in the database (if configured).

NOTE: Data is collected from all systems, even those without Intel AMT. Intel SCS tries to acquire data about Intel AMT using the Intel Manageability Engine Interface (Intel MEI) driver. If this driver is not installed and/or enabled, data is taken from the BIOS. If the manufacturer has not installed the correct BIOS in the platform, this can cause incorrect values in the data collected.

3.2 Using the Configurator

Download the entire Intel SCS package from http://intel.com/go/scs. Extract the Configurator directory, as selected in the example below and copy to the Intel AMT system.

On the Intel AMT system, open a command prompt to the Configurator directory.

NOTE: For systems running Microsoft Windows* 7, 8.1 or newer operating systems, this must be opened with elevated privileges due to interaction with a kernel level driver. This is done by right clicking on the executable and selecting “Run as administrator”.
The status command provides some basic information and determines the current Intel AMT configuration state:

```
ACUconfig.exe /output console status
```

In the above example, the output of the ACUconfig.exe Status command shows that the Intel(R) AMT version is 10.0.30, the system is un-configured and supports Host-Based Configuration.

When additional information is required across multiple systems in the environment, the `SystemDiscovery` command may be preferred as it can optionally capture information to a local file, Windows registry or send data to the Remote Configuration Service (RCS).

At the same command prompt, run the following:

```
ACUconfig.exe SystemDiscovery
```

This creates a local XML file and saves the data to the registry. The location for 32-bit and 64-bit Windows operating systems is:

- **HKLM\SOFTWARE\Intel\Setup and Configuration Software\SystemDiscovery**

In addition, on 64-bit operating systems:

- **HKLM\SOFTWARE\Wow6432Node\Intel\Setup and Configuration Software\SystemDiscovery**

The resulting data provides an in-depth view of the Intel AMT platform in a format which can be centrally collected via custom inventory solutions. Figure 3 shows the resulting XML file located in the Configurator directory and a preview of the file contents. The combined information is helpful with initial configuration and when troubleshooting is required.
For additional detail about the data collected, please refer to the Intel SCS User Guide section "Verifying the Status of Intel AMT"

3.3 Using the SCS_Discovery Utility

Another Intel SCS component is the standalone utility SCSDiscovery.exe, located in the SCS_Discovery folder. The Configurator and the Discovery Utility return exactly the same data, however the option to send the discovery data to the RCS and save it in the database is not available.

For additional detail refer to the Intel SCS User Guide section “Discovering Systems” and the “Intel SCS Discovery Utility” documentation, as detailed above.
3.4 Using the RCS

When the RCS is installed in database mode, you can send data discovery queries from to single or multiple systems. The Console sends a request to RCS to run remote discovery against specified systems. The RCS uses the WS-Man interface to gather Intel AMT related data from systems and saves this to the database. The RCS Console can be used to view the data collected for each system. For additional detail refer to the Intel SCS User Guide section “Viewing Discovery Data.”

3.5 Using the Platform Discovery Utility

The Platform Discovery Utility (PlatformDiscovery.exe) is used to interrogate the platform and identify available Intel platform products and capabilities. It returns data about the hardware and software for each Intel product on your Intel AMT system and you can use this data to determine what to enable and if any software or hardware updates are required. For more information, refer to the documentation in the Solutions_Framework folder.

3.6 Using the Solutions Framework

This is not covered in this guide. For more information, please refer to the documentation in the Solutions_Framework folder.
4 Configuration

4.1 Introduction

The factory default state for Intel AMT firmware is un-configured. This ensures un-authorized users cannot access the manageability and security features of Intel AMT. The three main objectives of the setup and configuration process are:

- Securely deliver an encrypted profile to the target AMT firmware.
- Enable Intel AMT features and specify behavior.
- Ensure that only authenticated and authorized users can access.

4.2 Configuration Methods

This section helps to determine which of the most common Intel AMT configuration methods is most appropriate and provides step-by-step instructions so that you can begin using Intel AMT. These include Host-Based Configuration, Manual Configuration and Remote Configuration using Public Key Infrastructure (PKI).

The decision tree below provides a simple flow to aid in the selection of a configuration method, all of which result in a configured Intel AMT system.
4.3 **Host-Based Configuration**

Host-Based Configuration (HBC) is the recommended configuration option and is supported from Intel AMT Release 6.2. HBC requires Windows Administrator permissions and by default puts the device into Client Control mode (CCM). CCM disables sensitive capabilities such as network filtering and requires mandatory user consent for Intel AMT Redirection and Boot Device Control Operations. This means the user must provide a random hardware generated 6-digit code that is displayed on the Intel vPro system, before a remote Intel AMT session can be established. Additional information is available in the Intel SCS User Guide, in the "Configuration Methods and Intel AMT Versions" and “Control Modes” sections.

4.4 **Using the Intel AMT Configuration Utility Wizard**

Below you'll find basic instructions for enabling Host-Based Configuration on your Intel AMT system using the Intel AMT Configuration Utility. This is a wizard based application that can be used to configure Intel AMT in two different ways:

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

2. Extract the ACU_Wizard directory, as selected in the example below and copy to the Intel AMT client.

```
Folders in WinZip File
[IntelSCS_10.0.11.35.zip]
  IntelSCS
    ACU_Wizard
    Configurator
    Licenses
    RCS
    sample_files
    SCS_Discovery
    Solutions_Framework
    Utils
```

3. On the Intel AMT system, navigate to the ACU_Wizard directory and select the executable `ACUWizard.exe`.

**NOTE**: For systems running Microsoft Windows* 7, 8.1 or newer operating systems, this executable must be opened with elevated privileges due to interaction with a kernel level driver. This is done by right clicking on the executable and selecting “Run as administrator”.

4. When the GUI is displayed, select **Configure/Unconfigure this system**.

5. Select “**Configure via Windows**”. In the bottom right hand corner you will see that Intel AMT is not configured on this system. Additional system details can be found by clicking the **System Info...** button.
6. For new Intel AMT systems the current password is **Admin**. Enter a new password and confirm. The existing configuration details should suffice.

![Image 1](image1.png)

**NOTE:** The password must be at least 8 and at most 32 characters long, must have at least 1 digit and 1 non-alphanumeric characters and both lowercase and uppercase Latin letters. The underscore (_) character is counted as alphanumeric.

7. The XML profile that is created as part of the configuration process contains sensitive data and the resulting file will be encrypted with a password using the following:
   - 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

![Image 2](image2.png)

**NOTE:** You can use the **SCSEncryption.exe** utility located in the Utils folder of the Intel SCS download package to encrypt and decrypt files using the same format used by Intel SCS. For more information, refer to the CLI help of the **SCSEncryption.exe** utility.

8. Click the **Configure** button and Intel AMT will begin configuration.
9. When the Intel Management and Security (IMSS) system tray applet dialog appears, the Intel Management Engine (Intel ME) configuration is complete.

![Intel® Management and Security Status](image)

10. For systems with AMT Release 10.0 the following configuration notification will also be shown.

![Intel® ME Configuration Notification](image)

11. For troubleshooting purposes you can locate this operation located in the ACU_Wizard directory. Additionally you'll find the encrypted file, `profile.xml` located in the same directory, which is protected with the password entered in step 7.

### 4.5 Using the Intel AMT Configuration Utility Command Line Interface (CLI)

1. Locate the Configurator directory created in section *Using the Configurator*.
2. Copy the file `profile.xml` file from the ACU_Wizard directory to the Configurator directory on the target Intel AMT system.

**NOTE:** For systems running Microsoft Windows* 7, 8.1 or newer operating systems, this executable must be opened with elevated privileges due to interaction with a kernel level driver. This is done by right clicking on the executable and selecting “Run as administrator”.

3. Open a command prompt on the Intel AMT system, using *Run as Administrator*.
4. Change to the Configurator directory and run the following command on the Intel AMT system (where `/DecryptionPassword` is the password entered when creating the original profile).

   ```
   ACUconfig ConfigAMT profile.xml /DecryptionPassword P@ssw0rd
   ```

5. When the Intel Management and Security (IMSS) system tray applet dialog appears, the Intel Management Engine (Intel ME) configuration is complete.

![Intel® Management and Security Status](image)
For troubleshooting purposes you can locate the log corresponding with this operation **ACU_Wizard** directory. Additionally you'll find the encrypted file, **profile.xml** located in the same directory, which is protected with the entered password.

**NOTE:** Once a single Intel AMT system has been configured and functionality validated, then the configuration directory containing the files ACU.DLL, ACUConfig.exe and the XML profile can be packaged up and using the above command can be distributed to all Host-Based Configuration capable Intel AMT systems within the target environment.

### 4.6 Manual Configuration

Host-Based Configuration (HBC) remains the recommended option and by default places the device into Client Control mode (CCM). The manual configuration method lets you configure an Intel AMT system with basic settings but it does require touching the device (to insert the USB key). However this puts Intel AMT into Admin Control Mode (ACM) and as such provides access to all AMT features, without the mandatory requirement for user consent.

**NOTE:** This option is only available on Intel AMT systems with AMT Release 4.0 and higher.

Detailed instructions for performing Manual Configuration are provided in the Intel SCS User Guide. The following is a summarized version.

1. From the Configuration Options window, select **Configure via USB key**.

2. Click on the **Next** button.

3. In the MEBx Password section, enter the password for the Intel MEBX

   - **Current Password**: The default password of un-configured systems ("admin") is automatically entered in this field. If this is not the password in the Intel MEBX, enter the correct password or configuration will fail.
   - **New Password**: For the first configuration it is mandatory to change the Intel MEBX password. For reconfiguration you must also enter a value
here which can be the same as the Current Password.

NOTE: The password must be at least 8 and at most 32 characters long, must have at least 1 digit and 1 non-alphanumeric characters and both lowercase and uppercase Latin letters. The underscore (_) character is counted as alphanumeric.

4. (Optional) Select Display advanced settings to view or edit the default settings that the Configuration Utility will define for this system.

5. **Power Settings**: Defines in which power states (of the host system) the Intel AMT device will operate.

6. The previous image shows the recommended setting. When the system is connected to power, all Intel AMT manageability features remain available in any of the system power states. If set to “Host is On (S0)” then Intel AMT manageability features are only available only if the operating system is up and running.

**Network Settings**: The recommended default setting is to configure the Intel AMT device with the hostname and the domain name defined in the operating system and to use the Dynamic Host Configuration Protocol (DHCP) server to configure the IP address of the device.
Redirection Settings: These settings are only shown for systems with Intel AMT 6.0 and higher.

7. Keep the default settings of Enable KVM Redirection to support KVM redirection and Allow IT to change user consent setting which allows to the user consent setting to be set remotely.

8. Now insert a USB key into the Intel AMT system and select the drive letter.

9. Click the Next button and a message is displayed warning that the USB key will be formatted.

10. Click the Yes button and 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.

11. Click the Finish button and the Configuration Utility closes.

12. Ensure that only the USB key that you created is connected to the target Intel AMT system and reboot.

13. During the reboot, a message is shown on the screen:

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

14. 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...

15. Remove the USB key and press a key to continue booting. The Intel AMT system is now configured and can be accessed remotely.

**NOTE:** After configuration, all data in the Setup.bin file on the USB key is deleted, however the file is not deleted. You must repeat all previous steps for each system that you want to configure using a USB key.

4.7 Manual Configuration (Multiple Systems)

Alternatively 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.
The Intel AMT Configuration Utility allows you create profiles with configuration settings for multiple systems. Select “Create Settings to Configure Multiple Systems” and the Profile Designer opens. Select Tools > Prepare a USB Key for Manual Configuration.

4.8 Remote Configuration Using PKI

This is the most comprehensive configuration method and remotely enables access to all Intel AMT capabilities (Admin Control Mode) without the mandatory requirement for user consent that comes with Host-Based Configuration (Client Control mode).

Dependent upon AMT Release, the Intel AMT firmware contains root certificate hashes from a number of commercial Certificate Authorities including Starfield, GoDaddy, Verisign, Comodo, EnTrust, Baltimore CyberTrust, GTE CyberTrust, Verizon etc. You can also add your own root certificate hash into the Intel MEBX.

To support Remote Configuration using PKI, an SSL certificate from one of these embedded hashed root certificates must be purchased from a commercial SSL certificate provider. This is often referred to as a Remote Configuration (RCFG) or Provisioning certificate and is used by the RCS to authenticate with Intel AMT systems. Acquiring this SSL certificate is a multi-step process and defined in section 6 which also covers Remote Configuration Using PKI.

NOTE: Remote Configuration Using PKI is an advanced configuration option. Host-Based Configuration (HBC), supported from Intel AMT Release 6.2 remains the recommended configuration option, if mandatory user consent requirement for re-direction operations is acceptable.

4.9 Unconfigure Method

This simplest method to un-configure or un-provision AMT is to utilize the Intel AMT Configuration Utility Wizard.

1. Extract the ACU_Wizard directory, as selected in the example below and copy to the Intel AMT system.

2. On the Intel AMT system, navigate to the ACU_Wizard directory and select the executable ACUWizard.exe.

NOTE: For systems running Microsoft Windows* 7, 8.1 or newer operating systems, this executable must be opened with elevated privileges due to interaction with a kernel level driver. This is done by right clicking on the executable and selecting “Run as administrator”.
3. When the GUI is displayed, select **Configure/Unconfigure this System**.

4. Select **Unconfigure** and click the **Next** button.

5. Select **Unconfigure this system using admin password**, enter the admin password (P@ssw0rd) and click the **Next** button.
6. Once complete AMT will be un-configured and un-provisioned. Click the **Finish** button.

7. The Intel Management and Security Status will also display that the **Intel ME is Unconfigured**.
5 Install and Configure Intel RCS and Console

As discussed in the “Intel® Setup and Configuration Software (Intel® SCS) Overview” section of this guide, there are numerous components available within the Intel SCS download package.

The RCS is used to remotely configure and maintain (when a Database is available) Intel AMT systems and is a Windows based service (RCSServer) that runs on a computer in the network.

The RCS and console components should be installed and configured and an AMT provisioning certificate purchased if you want to do any of the following:

- Place Intel AMT devices into Admin Control Mode (ACM)
- Use the Remote Configuration approach
- Use the One-Touch Configuration approach
- Use Digest Master Passwords
- Use the Solutions Framework to publish data to the RCS

You do not need the RCS, console or AMT provisioning certificate if you want to configure Intel AMT systems in your environment using one of these approaches:

- Manual Configuration
- Host-based Configuration (Client Control Mode)

For the purposes of this guide, Intel SCS will be installed in Non-Database Mode with the Remote Configuration Service (RCS) and console installed locally. In this mode, the RCS does not store data about the Intel AMT systems. Configuration and maintenance tasks can only be done using the Configurator. This mode is not supported by the Solutions Framework.

More information is available in “Setting up the RCS” and “Selecting the Type of Installation” sections within the Intel SCS User Guide.
1. From the RCS directory run the executable IntelSCSInstaller.exe. The Welcome window opens. Click the Next button.

2. Select I accept the terms of the license agreement and Click the Next button.
3. Ensure the **Remote Configuration Service (RCS)** and **Console** are selected. The **Non-Database Mode** is optional and for this guide the Database Mode option is not selected. Click the **Next** button.

4. The Windows operating system includes a built-in security account named "Network Service". This account increases security as it is not easy to impersonate a computer and it is recommended to run the RCS using this built-in security account. The Network Service account does not require a password. Click the **Next** button.
5. The Storage Encryption Key window opens. This will install the encryption key for the RCS to use when accessing the data files. Select the option to “Generate storage key file” to automatically create and install the storage encryption key. Click the Next button.

![Storage Encryption Key](image1)

**NOTE:** If you selected the Generate storage key file option you must create a backup of the storage encryption key that the Installer created and installed automatically. You can export this encryption key to a file, as described in the Intel SCS User Guide section “Moving the RCS to a Different Computer.”

6. Click the Next button. The Confirmation window opens and shows information about the selections made. The default installation folder is C:\Program Files\Intel\SCS10. If you want to change the location, type a new path in the Install path field or click the Browse button to select it.

![Confirmation](image2)
7. Click the **Install** button. The Installation Progress window opens. When installation is complete, a message is shown.

![Installation Progress](image1)

8. Click the **Next** button. The Completed Successfully window opens. Click the **Finish** button. The Installer closes. The RCS is now installed with default settings. If necessary, you can change these settings (see Defining the RCS Settings within the Intel SCS User Guide).

![Completed Successfully](image2)
6 Intel AMT Provisioning Certificates

6.1 Introduction

This SSL certificate, commonly referred to as the Remote Configuration certificate (RCFG) or AMT provisioning certificate is used to establish initial trust between the Intel RCS and Intel AMT systems when initiating client configuration into Admin Control Mode.

Dependent upon AMT Release, the firmware contains root certificate hashes from a number of commercial Certificate Authorities including Starfield, Go Daddy, Verisign/Symantec, Comodo, EnTrust, Baltimore CyberTrust, GTE CyberTrust, Verizon etc. See the table below for details. From AMT Release 7.0 you can add your own root certificate hashes into the Intel MEBX (up to 10 custom SHA1 hashes).

To support Remote Configuration using Public Key Infrastructure (PKI), a suitable SSL certificate must be purchased from one of the commercial SSL certificate providers, whose hashed root certificates are embedded within Intel AMT firmware.

NOTE: Host-Based Configuration (HBC), supported from Intel AMT Release 6.2 or the Manual approach do not require an AMT provisioning certificate and HBC remains the recommended option, if mandatory user consent requirement for re-direction operations is acceptable.
This section provides simple, step-by-step instructions to obtain an AMT provisioning certificate suitable for use with remote configuration of Intel AMT systems using freely available OpenSSL tools.

The diagram below illustrates the necessary steps and overall flow to support this process, which consists of the following 5 high level steps:

1. **GENERATE** a certificate signing request (CSR) suitable for use by Intel AMT. This step includes creating the public and private keys.
2. **SUBMIT** request for a SSL certificate from a commercial Certificate Authority.
3. **ISSUE** a signed certificate, once procedural steps required by the CA have been completed.
4. **MERGE** the signed certificate with your private key.
5. **INSTALL** the resulting certificate into the RCS Local Machine certificate store.

**NOTE:** For evaluation purposes you can add your own root certificate hash into the Intel MEBX. However this is not recommended for large scale deployments and is not covered in this guide.

Before pursuing this approach consider Host-Based Configuration.

Additional information is available in the Intel SCS User Guide under the section “Setting up Remote Configuration”.

Start
Modify Certificate Signing Request Configuration File (AMT.CFG)
SAVE PRIVATE KEY
Submit CSR to CA (AMTCSR.PEM)
Generate Certificate Signing Request (MAKEAMTCSR.BAT)
Generate Private Key (AMTKEY.PEM)
CA Signed Certificate (AMTCERT.PEM)
Merge signed CA Certificate with the Private Key (MAKEPFX.BAT)
Intel AMT Remote Config Certificate & Password (AMTCERT.PFX)
Import Certificate & Password into RCS Personal Certificate Store (RCSUTIL.EXE)
Provision Intel AMT using Intel SCS client tools (ACUCONFIG.EXE)
Alternative guides are available on how to purchase and install certificates below.

<table>
<thead>
<tr>
<th>Certificate Authority</th>
<th>URL</th>
</tr>
</thead>
</table>

6.2 Prerequisites

Download the OpenSSL tools for Microsoft Windows from the URL below and copy into a folder on a Windows client.

http://www.openssl.org/related/binaries.html

NOTE: Select the pre-compiled Win32/64 libraries without external dependencies and choose download the zip file.

Create two batch files, MAKEAMTCSR.BAT and MAKEPFX.BAT using the reference section below and save these into the OpenSSL folder.

6.3 Reference

MAKEAMTCSR.BAT
openssl req -config AMT.CFG -new -keyout AMTKEY.PEM -out AMTCSR.PEM -days 365

MAKEPFX.BAT
openssl pkcs12 -export -in AMTCERT.PEM -inkey AMTKEY.PEM -out AMTCERT.PFX -name "Intel(R) RCFG Certificate" -password "pass:P@ssw0rd"

NOTE: This example includes a password P@ssw0rd to protect the private key. Ensure you make a note of this you change it.

AMT.CFG
# Sample OpenSSL configuration to generate a certificate request
# (CSR) for an Intel(R) AMT(tm) Provisioning Certificate
# Provide the output file AMTCSR.PEM file to your Commercial Certificate Authority

RANDFILE = /.rnd

# None of the fields in [ req ] section should be changed, except
# 'default_bits' which can be set to 1024, 1536 or 2048
# Supported key lengths are 1024 and 2048.
# The maximum key size supported by Intel SCS is 2048.
# SHA-1 is the only supported hash algorithm.
[ req ]
default_bits = 2048
default_keyfile = keyfile.pem
encrypt_rsa_key = no
default_md = sha1
req_extensions = req_extensions_section
prompt = no
distinguished_name = req_distinguished_name_section

# The C, ST, L, O fields below are mandatory and must exactly
# match the business registration details of the organisation
# requesting the certificate
#
# The OU field is mandatory and should not be changed
#
# The CN field is mandatory and should match the FQDN of the
# provisioning server. The DNS domain portion of the CN field
# must be owned by the organisation requesting the certificate
#
# The 'emailAddress' field is optional

[ req_distinguished_name_section ]
C = US
ST = California
L = San Francisco
O = My Company Inc
OU = Intel(R) Client Setup Certificate
CN = provisionserver.mydomain.com
emailAddress = administrator@mydomain.com

# None of the fields in [ req_extensions_section ] section should
# be changed unless requesting a Unified Communication Certificate
# (UCC). When requesting a UCC uncomment the 'subjectAltName' field

[ req_extensions_section ]
basicConstraints = CA:FALSE
keyUsage = digitalSignature
extendedKeyUsage = critical,serverAuth,2.16.840.1.113741.1.2.3
subjectKeyIdentifier = hash

# subjectAltName = @alt_name_section
# When applying for a Unified Communication Certificate (UCC),
# uncomment the entire [ alt_name_section ] section and set DNS.x
# entries to match additional domains. DNS.x entries can be added
# or removed. The DNS domain portion of DNS.x entries must be
# owned by the organisation requesting the certificate

# [ alt_name_section ]
# DNS.1 = provisionserver.mydomain.co.uk
# DNS.2 = provisionserver.mydomain.co.fr

## 6.4 Generate Certificate Signing Request (CSR)

To install a digital certificate, you must first generate a Certificate Signing Request (CSR) for the Certification Authority (CA).

The CSR contains your certificate-application information, including your public key. When you generate the CSR, you also create your public/private key pair which is used for encrypting and decrypting secure transactions.

1. Use the AMT.CFG example in the above reference section to create your own configuration file AMT.CFG in the OpenSSL folder.

2. Edit the section [req_distinguished_name] and modify the C, ST, L and O fields. Set these to the appropriate country, state or province, location, company name.

   **NOTE:** The company information must match the government or registered commercial company information.

3. Edit the CN field to correctly match the hostname and domain name of the server where Intel RCS is running. This is the fully qualified domain name (FQDN).

   **NOTE:** Do not change the OU field, this contains the appropriate OU that traces to a CA that has a root certificate hash stored in the Intel AMT device. The exact text string in English must be used, in the same case, without a trailing period. **OU = Intel(R) Client Setup Certificate**

4. Save the edited file AMT.CFG.

5. Run the batch file MAKEAMTCSR. This command generates the public key, private key AMTKEY.PEM and a CSR file named AMTCSR.PEM.

   **NOTE:** Ensure you safely store and backup the private key AMTKEY.PEM and the CSR file AMTCSR.PEM created in step 5.

## 6.5 Submit Certificate Signing Request (CSR)

Now that you’ve generated the CSR, you must request the SSL certificate. Then, complete the process by downloading and installing the certificate.

When requesting a SSL certificate from your CA you will be prompted for the CSR by the CA website. Cut and paste the contents of AMTCSR.PEM into the CA website dialog box. If you are asked what type of software you are using the certificate with, use Other. If you are asked for Cryptographic service provider, select **Microsoft Strong Cryptographic Provider**
6.6 Merge Issued Certificate

The procedural steps required by the CA vary, however expect to provide proof of domain ownership and proof of organizational details which may include providing commercial documents. You may also be contacted by the CA to verify commercial contact details. The CA should provide clear information on their website indicating what criteria needs to be satisfied before certificates can be issued.

You should receive a signed certificate from the CA which needs to be merged with the private key `AMTKEY.PEM` so this can be loaded into RCS's Local Machine certificate store. To carry out this process follow these instructions:

Copy the signed certificate from the CA into a file called `AMTCERT.PEM`. The file should have a format which starts with the string `---BEGIN CERTIFICATE---` and ends `---END CERTIFICATE---`.

Ensure `AMTCERT.PEM` is in the same directory as the private key `AMTKEY.PEM`. The `MAKEPFX.BAT` created earlier will merge the signed certificate from the CA with the private key and produce a file `AMTCERT.PFX`. The password protecting the private key is `P@ssw0rd`.

**NOTE:** The example `MAKEPFX.BAT` includes a password P@ssw0rd to protect the private key. Ensure you make a note of this if it's been changed.

You now have a SSL certificate suitable for use with Intel AMT and remote configuration that is in a format suitable for loading into the certificate store of your Microsoft Windows server running the Intel RCS.

6.7 Installing Root and Intermediate Certificates

The AMT provisioning certificate may have come from a CA whose signing chain is not automatically included in the trusted certificates store. The complete signing chain is required and as such it will be necessary to install the Root and Intermediate certificates in the RCS Local Machine Root and Intermediate stores of the RCS (`RCSServer.exe`).

1. Retrieve the Root and any Intermediate certificates, according to the instructions of the certificate vendor. For example it may be possible to download these from their website or they may email them. Save the certificates in `.CER` format.
2. Locate each stored certificate, right-click and select `Install certificate`. The certificate manager Import Wizard opens.
3. Click the `Next` button.
4. Select `Automatically select the certificate store based on the type of the certificate`. Click the `OK` button.
5. Click the `Next` button then click on the `Finish` button.
6. When prompted if you want to add the certificate to the root store, click the `Yes` button.
6.8 Install and Validate the Certificate

This guide uses the Network Service account to run the RCS and the AMT provisioning certificate must be installed into the local certificate store of the Network Service Account so it can access this certificate during the configuration process.

Since you cannot "logon" using the Network Service Account, Intel has developed the Remote Configuration Service Utility (RCSUtil.exe). This is a Command Line Interface (CLI) used to make RCS setup tasks easier including installing certificates and applying Windows Management Instrumentation (WMI) permissions to user accounts that require to access the RCS.

The RCS Utility (RCSUtils.exe) is located in the Utils folder within the Intel SCS download package and can be run from a command line prompt or using a batch file.

You must run the RCS Utility on the computer where the RCS is installed and running.

1. Copy the file AMTCERT.PFX into the Utils directory, you will also need the password that protects the private key (P@ssw0rd).
2. Open a command prompt on the Intel AMT system, using Run as Administrator.

```
NOTE: For systems running Microsoft Windows* 7, 8.1 or newer operating systems, this executable must be opened with elevated privileges due to interaction with a kernel level driver. This is done by right clicking on the executable and selecting "Run as administrator".
```

3. Change directory to the Utils folder.
4. To install the AMT provisioning certificate into the certificate store of the Network Service account running the RCS, run the following command:
   ```
   RCSUtils.exe /Certificate Add AMTCERT.PFX P@ssw0rd /RCSUser NetworkService /Log File AddCert.log
   ```
5. The following command is used to view the AMT provisioning certificate and its complete chain and if these were imported successfully:
   ```
   RCSUtils.exe /Certificate View /RCSUser NetworkService /Log File ViewCert.log
   ```
NOTE: The RCS Utility uses the Windows Task Scheduler to impersonate the Network Service account. To do this, a task is created and run immediately. The results from this task cannot be sent to the console screen so the log option is used.

6. You will see your AMT Provisioning Certificate with its thumbprint (hash) listed. This is required to validate the certificate and signing chain for remote configuration in the step below.

   RCSUtils.exe /Certificate Validate
   F779AC7B8D35CE381BDAB20AE25B1C864B3F599 /RCSUser
   NetworkService /Log File ValidateCert.log
View the resulting log file identifies the complete certificate chain and provides a message that the certificate is valid for Intel RCS Remote PKI.
6.9 Verify and Validate Remote Configuration Using PKI

Remote configuration of Intel AMT is performed Out of Band via the on-board Intel wired LAN interface. Enterprise wired environments provide the best environment when using Intel AMT and is recommended for initial testing and deployment.

To support remote configuration using PKI all the Intel AMT systems to be provisioned should be directly connected to the enterprise via the wired LAN interface (not via VPN or using an Ethernet dongle).

This presents problems for some of the latest Intel vPro mobile platforms that do not include an onboard wired LAN interface, only a wireless interface. Intel AMT Release 9.x systems cannot be configured entirely remotely, however Intel AMT Release 10.x systems fully support remote configuration. The configuration of these LAN-less Platforms is covered in the Wireless section.

6.9.1 Create AMT Profile

1. Within the Intel SCS Console, create a new profile.
2. In the Profile Wizard window, give the profile a name (profile).
3. Click the Next button and leave all Optional Settings unselected.
4. Click the Next button.
5. In the System Settings screen, provide the following settings.
   - **Enable option:** ME will go into lower power state when idle
   - **Set Timeout if Idle** to 65535
   - **MEBx Password:** P@ssw0rd
   - **Intel AMT Admin Password:** P@ssw0rd
   - **Enable** Intel® AMT to respond to ping requests
6. Click the OK, Next, and Finish buttons to complete the profile.
6.9.2 Apply AMT Profile

1. Extract the Configurator directory from the Intel SCS package, as selected in the example below and copy to the Intel AMT client.

![Folder structure showing Configurator directory](image)

2. Open a command prompt on the Intel AMT system, using Run as Administrator and change to the Configurator directory.

3. Run the following command:
   
   ```
   ACUConfig.exe ConfigViaRCSonly RCS Server IP Address or FQDN profilename
   ```

   **NOTE:** More information on the ACUconfig.exe ConfigViaRCSonly command is available in the “Configuring Systems Using the RCS” section of the Intel SCS User Guide.

4. When the Intel Management and Security (IMSS) system tray applet dialog appears, the Intel Management Engine (Intel ME) configuration is complete.

6.10 Verify AMT Connectivity

1. To verify configuration of Intel AMT on the managed client, perform the following from the open command prompt in the Configuration directory:
   
   ```
   ACUconfig.exe /output console status
   ```

2. The screen below shows the system is now configured in Admin Control Mode.

![Command output showing system configuration](image)

3. From the SCS console system, open a web browser and enter the URL for the Intel AMT System: [http:// FQDN:16992](http://FQDN:16992)
4. If the Intel AMT on page displays, the managed client is configured.
5. Click the Log On button.

![Image of Intel Active Management Technology](image)

6. Enter the default user “admin” and the password set using the profile, P@ssw0rd.
7 Microsoft Active Directory

7.1 Introduction

This is an optional feature that provides the capability for Intel AMT to be integrated with the security infrastructure of your network's Microsoft Active Directory (AD). This integration includes the ability to:

- Support Single Sign On using Microsoft Windows domain user and group accounts when interacting with Intel AMT systems.
- Use the 802.1x protocol for wired and wireless access.
- Use End-Point Access Control (EAC).

**NOTE:** 802.1x and EAC are beyond the scope of this deployment guide.

When AD integration is enabled, during configuration Intel SCS will send a request to create a Computer object for the Intel AMT system to support Kerberos authentication. By default, the AD Computer object is created with a User Principal Name (UPN) that matches the hostname of the Intel AMT system as defined in the Intel SCS configuration profile and the operating system (with $iME appended). Each Intel AMT system is recorded in the Active Directory database as an Intel AMT object and defined as an AD Computer object with the version of Intel AMT linked to it. AD uses the Intel AMT device password to create the device secret. During un-configuration of AMT a request to delete the AD Computer object is performed.

**NOTE:** Prior to Intel SCS version 9.1 this object could be detected as a User Object by some applications that calculate their license fee based upon the number of User Objects in AD. Changes in Intel SCS 9.1 ensured the object created is always detected as a Computer Object.

The Intel AMT system will register and authenticate with Active Directory after it has booted and provides six Service Principal Names (SPNs) for the six services it provides:

<table>
<thead>
<tr>
<th>SPN</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP/FQDN:16992</td>
<td>SOAP over HTTP</td>
</tr>
<tr>
<td>HTTP/FQDN:16993</td>
<td>SOAP over HTTPS</td>
</tr>
<tr>
<td>HTTP/FQDN:16994</td>
<td>Redirection over TCP</td>
</tr>
<tr>
<td>HTTP/FQDN:16995</td>
<td>Redirection over TLS</td>
</tr>
<tr>
<td>HTTP/FQDN:623</td>
<td>DMTF manageability over TCP</td>
</tr>
<tr>
<td>HTTP/FQDN:664</td>
<td>DMTF manageability over TLS</td>
</tr>
</tbody>
</table>
NOTE: Deleting the AD object of a configured Intel AMT system causes Kerberos authentication to fail and blocks access to Intel AMT using Kerberos admin user accounts. If you also do not know the password of the Digest admin user, this will make it impossible to remotely access or reconfigure Intel AMT.

7.2 Prerequisites

To implement Active Directory integration the Intel AMT system must be joined to the domain and have an associated Computer object.

For additional detail refer to the Intel SCS User Guide section “Defining Active Directory Integration”.

7.2.1 Create New OU

To separate the two Computer objects, it is best practice to create a separate Active Directory Organization Unit (OU) to store Intel AMT Computer objects. Control of this OU must be assigned to the service account running the RCS. Within this deployment guide the account used is NT AUTHORITY\NetworkService and is a member of the AMT Administrators domain group.

7.2.2 Create New AD Groups

Up to 32 Active Directory users/groups can be configured with suitable permissions to access common Intel AMT features. It is highly recommended that specific AD Domain groups are created to support roles such as Administrators, Support Engineers, Service or Help Desk with permissions assigned based upon the requirements of specific group in particular customer environments. Some examples follow.

**AMT Administrators**: Members of this group have full administration access to all AMT features over both interfaces (out of band and local) Associate the AMT “PT Administration” Realm with the “Domain Admin” AD group and define “Both” as the access type.

**AMT Provisioners**: Members of this group can provision Intel vPro clients. Associate the AMT “PT Administration” Realm with AD group members including “Domain Admin”, “Domain Computers” and the Computer object representing the Network Service account running the RCS with the access...
Service Desk: Access is limited to the following Realms over both interfaces to support the majority of standard vPro use cases:

- Redirection
- Hardware Asset
- Remote Control
- Event Manager
- General Info
- Event Log Reader

AMT Auditors: The access monitor can be used to monitor and audit attempts to execute damaging actions and is implemented by means of two elements: an Audit Log and a special Auditor user that you assign to the Access Monitor realm. You can assign the Access Monitor realm to one user only, and only that user can relinquish it. By default, the default admin user account has access to this realm.

7.2.3 Create New Local Groups

In addition to the AD groups, create the following local groups on the server running the RCS:

- RCS Admins has access to all RCS namespaces. Members of this group are typically “Domain Admins”.
- RCS Users only has access to Intel_RCS namespace. This is necessary for the user account using ACUConfig.exe when provisioning.

It is best practice to ensure that the “RCS Admins” local group has access to all RCS WMI namespaces.

This is easily done using the RCS Utility (RCSutils.exe) which is located in the Utils folder within the Intel SCS download package and must be run from a command line prompt on the computer where the RCS is installed and running.

1. Open a command prompt on the Intel AMT system, using Run as Administrator.

2. Change directory to the Utils folder.

3. Run the following command lines:

   RCSUtils.exe /Permissions Add “RCS Admins” /RCSnamespace All
   RCSUtils.exe /Permissions Add “RCS Users” /RCSnamespace RCS

**NOTE:** For systems running Microsoft Windows* 7, 8.1 or newer operating systems, this executable must be opened with elevated privileges due to interaction with a kernel level driver. This is done by right clicking on the executable and selecting “Run as administrator”.
7.2.4 Assign Permissions to New OU

The basic permissions for the OU used during the AMT provisioning process are for the previously created AD Group AMT Provisioners:

- This object only: Create Computer Objects and Delete Computer Objects and List content (default).
- Descendant Computer Objects: Full Control.

Check the box Apply these permissions to objects and/or containers within this container only and click the OK button.

The latter permissions for Descendant Computer objects may not be acceptable and can be trimmed down for the AD Group AMT Provisioners to include only Change password and Write all properties.

7.3 Verify and Validate Microsoft Directory Integration

7.3.1 Create AMT Profile

Follow the steps as defined in the Install and Validate the Certificate section to create a new profile, named BasicADProfile.
1. In the **Getting Started** window select **Configuration/Reconfiguration**
2. Click the **Next** button and select the **Optional Settings** window with the following options:
   - **Active Directory Integration**
   - **Access Control List (ACL)**

   ![Configuration Profile Wizard Basic ADProfile](image)

   Select the settings that you want to configure. Unconfigured settings that are not selected will be removed from the system during configuration.
   - **Active Directory Integration**
     - Allow Intel® AMT access to Active Directory features
   - **Access Control List (ACL)**
     - Assign each access level to the system based on users and groups
   - **Hidden Domain**
     - Define trusted domains where the Intel® AMT functionality will be available
   - **Network Access**
     - Enable (all) all network communication with remote management via a Management's Resource Server (MRS)
   - **Transport Layer Security (TLS)**
     - Use the TLS protocol to encrypt and authenticate communication with the domain
   - **Network Configurations**
     - Select at least one of the following options:
       - WPN Connections
       - Wired 802.1x Authentication
       - wipe settings for wipe (W) only
       - NTLM: Additional Access Control (DAC)
     - Set wipe or other system states

**NOTE:** If the AD OU was not created in the previous section and no create/delete rights were granted to the OU as described in the previous section, do not select Active Directory Integration. You can only be using Digest User for authentication.

In the Active Directory OU box, locate the **Out of Band Management Controllers** AD OU previously created, click the **OK** button and then the **Next** button.

In the ACL Window, click the **Add** button, select **Active Directory User/Group** and click the **Browse** button to one of the AD groups previously created i.e. **AMT Provisioners** and select **Both** to set the Access Type to access all AMT features over both interfaces (out of band and local). By selecting PT Administration members of the **AMT Provisioners** group will have full access to all AMT capabilities on the Intel AMT system. Click **OK**. Repeat for other AD groups who will require access.
7.3.2  Apply AMT Profile

Open a command prompt on the Intel AMT system, using *Run as Administrator* and change to the Configurator directory and execute the following command:

```
ACUconfig.exe ConfigViaRCSonly RCS Server IP Address or FQDN BasicADprofile
```

**NOTE:** If you are using Host-Based Configuration then export the profile to an XML file from the Intel SCS Console, copy to the Intel AMT system and run the following command:

```
ACUconfig.exe ConfigAMT BasicADprofile.xml /DecryptionPassword P@ssw0rd
```

7.3.3  Verify AMT Connectivity

From the SCS console system, open a web browser and enter the URL for the Intel AMT System: **http://FQDN:16992**

If the Intel AMT on page displays, the managed client is configured.

```
Intel® Management and Security Status
Intel® ME is Configured. Reboot is required.
```

If you are logged as a Domain User who is a member of one of the groups then clicking Log On will provide authorized access to Intel AMT.

**NOTE:** When testing against the Intel AMT WebUI using Microsoft Internet Explorer, a change to the Windows registry is required to enable Kerberos authentication over non-standard HTTP ports such as 16692/16993. More information is available in the Post-Hotfix section of Microsoft KB908209: http://support.microsoft.com/kb/908209.
8 Secure Communications Using Transport Layer Security (TLS)

8.1 Introduction

Intel AMT uses digital certificates for encryption and authentication purposes and to unify the certificates usage model all certificates are stored in the Intel AMT certificate store.

NOTE: For additional information on Intel AMT certificate management features please see the following:

TLS is an optional feature that secures management traffic between the Intel AMT system and RCS and integrates with the Public Key Infrastructure (PKI) of an organization. Its implementation should be evaluated based upon your environment and security policies. A Certificate Authority (CA) is necessary if you want to configure any of these settings in an Intel AMT system:

- Transport Layer Security
- Remote Access
- Use the 802.1x protocol for wired and wireless access
- Use End-Point Access Control (EAC)

NOTE: Remote Access, 802.1x and EAC are beyond the scope of this deployment guide.

During configuration of the Intel AMT system the RCS sends a request to the CA to generate a certificate and places this into the firmware of the Intel AMT system. The RCS can request certificates from:

- A Microsoft* CA (Default option)
- Via a CA Plugin (optional plugin required, not covered in this guide)

Management consoles such as McAfee* Deep Command and Microsoft* System Center Configuration Manager require TLS to interact with Intel AMT systems.

NOTE: For additional detail refer to the Intel SCS User Guide section “Preparing the Certification Authority”.

8.2 Prerequisites

Intel SCS supports the Standalone and Enterprise versions of Microsoft CA. The Microsoft PKI may have a hierarchy of CAs, with subordinates and a root. This is beyond the scope of this guide.

The following features require either a Standalone or an Enterprise root CA:

- Transport Layer Security
- Remote Access with password-based authentication
These features require an Enterprise root CA:

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

Configuring TLS on an Intel AMT system requires a certificate to be configured on the CA. This certificate is a duplicate of the WebServer template with some modified properties. The private key of this certificate is requested and stored in the firmware during configuration of the Intel AMT system. The service account running the RCS must have the following permissions on the CA:

- Issue and Manage Certificates
- Request Certificates

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

Within this deployment guide the account used is NT AUTHORITY\NetworkService.

8.2.1 Request Handling

When requesting a certificate the RCS does not handle pending requests so you need to check how these are handled. If during configuration the CA places the certificate into the “Pending Requests” state, Intel RCS will return an error 35. To ensure that the CA and the templates used by Intel RCS do not do this, check the Request Handling properties of the Policy Module tab on CA as shown below.

8.2.2 Create Certificate Template

If you are using Intel RCS with an Enterprise CA to configure Intel AMT features to use certificate-based authentication, you must define certificate templates. This section details the process using the Microsoft Management Console Certificate Templates plug-in to define the correct settings for Intel AMT.

NOTE: Certificate Revocation Lists (CRL) are not covered in this section and Intel RCS does not use the original CRL file supplied by the Certification Authority. Additionally CRL is only available to
1. From your Certificate Authority, run the Microsoft Management Console with the Certificate Templates plug-in.

2. Expand the CA, right-click Certificate Templates, and select Manage to load the Certificate Templates management console.

3. In the right-pane, right-click the Web Server template and select Duplicate Template.

4. The Duplicate Template Window asks if you want to create a certificate template for Windows Server 2003 Enterprise or for Windows Server 2008 Enterprise. Select Windows Server 2003 Enterprise and click OK.

**NOTE:** Only version 2 certificate templates are supported. Version 3 certificate templates (Windows Server 2008) cannot be selected in the configuration profile.

### 8.2.3 Configure Certificate Template

1. At the Properties of New Template dialog, click the General tab and enter a name i.e. AMT Web Server Certificate, into the Template display name field.

2. Ensure that the Publish certificate in Active Directory check box is **NOT** selected. For settings specific to your organization, such as certificate validity and renewal periods, specify the required values.
3. Click the **Request Handling** tab and ensure the Minimum key size field is not assigned a value higher than **2048**, which is the maximum key size supported by Intel SCS. Additionally ensure the **Allow private key to be exported** check box is selected.

4. Click the **CSPs** button.
5. In the list of requests, select the **Microsoft Strong Cryptographic Provider** check box and click the **OK** button.

8.2.4 **Assign Permissions to Certificate Template**

1. Click the **Security** tab. Select the Domain Admins and Enterprise Admins groups and uncheck Allow **Enroll** permissions for both these.
2. Click **Add** to add the **AMT Provisioners** group and check **Allow Read and Enroll permissions for this group**. Click on the **OK** button.
8.2.5  Issue Certificate Template

1. At the CA management console, right-click Certificate Templates and click New Certificate Template to Issue.
2. In the Enable Certificate Templates dialog, select the **AMT Web Server Certificate** template just created and click OK to enable certificates to be created based on this template.

![Certificate Authority Console](image)

3. Do not close the Certificate Authority Console.
4. At the CA Console, right-click the CA, in this example **vProLab Enterprise Issuing CA** and click Properties.
5. Click on the **Security** tab in the CA Properties Window.
6. Click **Add** to add the **AMT Provisioners** group and Allow **Issue** and Manage **Certificates** and Request **Certificates** permissions for this group. Click the **OK** button.

7. Close the Certificate Authority Console.

8. Restart the CA to publish the new template in Active Directory.
8.3 Verify and Validate Transport Layer Security (TLS) Configuration

8.3.1 Create AMT Profile

1. Follow the steps as defined in the Install and Validate the Certificate section to create a new profile, name this BasicTLSProfile.
2. In the Getting Started window select Configuration/Reconfiguration.
3. Click on the Next button and select the Optional Settings window with the following option:
   - Transport Layer Security

   ![Optional Settings](Image)

   Select the settings that you want to configure. On configured systems, settings that are not selected will be removed from the system during configuration.

4. Select Next, then the method for creating the certificate that will be installed in the Intel AMT system from the drop-down list. Default is Request certificate from Microsoft CA.
5. If a Microsoft Enterprise CA was used and you configured access as described earlier, the pull down list will automatically populate with registered CA’s for your environment. Intel SCS automatically detects if the selected CA is a Standalone root CA or an Enterprise root CA.
6. From the Server Certificate Template drop-down list, select the template that you previously defined for TLS i.e. AMTWebServerCertificate shown below.

7. Leave System Settings as previously defined in the Install and Validate the Certificate section and click on the Finish button.

8.3.2 Apply AMT Profile

1. Open a command prompt on the Intel AMT system, using Run as Administrator, change to the Configurator directory and execute the following command:

   ACUconfig.exe ConfigViaRCSonly RCS Server IP Address or FQDN BasicTLSprofile

   NOTE: If you are using Host-Based Configuration then export the profile to an XML file from the Intel SCS Console, copy to the Intel AMT system and run the following command:

   ACUconfig.exe ConfigAMT BasicTLSprofile.xml /DecryptionPassword P@ssw0rd

2. When the Intel Management and Security (IMSS) system tray applet dialog appears, the Intel Management Engine (Intel ME) configuration is complete. Reboot if required (AMT 10 only).

8.3.3 Verify AMT Connectivity

1. From the SCS console system, open a web browser and enter the URL for the Intel AMT system: https://FQDN:16993
2. If the Intel AMT page displays, the managed client is configured.

**NOTE:** Once TLS is configured use HTTPS with the target IANA port of 16993 to access the Intel AMT system.

**NOTE:** When testing against the Intel AMT WebUI using Microsoft Internet Explorer, a change to the Windows registry is required to enable Kerberos authentication over non-standard HTTP ports such as 16692/16993. More information is available in the Post-Hotfix section of Microsoft KB908209: http://support.microsoft.com/kb/908209.
9 Wireless

9.1 Introduction

As new innovative Intel vPro form factors, designs and categories i.e. Ultrabook become mainstream these typically have no on-board wired LAN interface due to requirements around size, weight and thickness. These LAN-less platforms present challenges if you want to configure Intel AMT into Admin Control mode and they need to be handled differently to systems that have a built-in wired LAN interface. This is due to the Remote Configuration using PKI only being performed via Out of Band using the on-board wired LAN interface.

Traditionally this has meant that mobile platforms can only be remotely configured if in addition to the WLAN interface, they also have an onboard wired LAN interface that is directly connected to an organizations network (not via VPN). Alternatively you can configure LAN-less platforms into Client Control mode using the host-based configuration approach, with the mandatory user consent requirements.

Intel SCS 10 in combination with Intel AMT Release 10 now supports Remote Configuration using PKI (RCFG), with some pre-requisites and the flow chart in section 4.2 details the approach.

NOTE: Configuring LAN-less Systems via Manual mode is another option that is not covered in this deployment guide. Please reference the Intel SCS User Guide for additional detail.

9.2 Prerequisites

Configuration of Intel AMT over WLAN requires a Wi-Fi profile to be setup which is applied during configuration. The profile provides information including network keys, encryption and authentication protocol settings and other security elements to authenticate against an organizations wireless infrastructure. Additional requirements include:

- The Intel AMT system share its IP address with the host operating system and is configured to use DHCP.
- WLAN infrastructure that supports WPA or WPA2 wireless security.

The total number of Wi-Fi setups including 802.1x that can be configured depends on the version of Intel AMT. For 8.x and lower, a maximum of 15. AMT 9.0 and higher, a maximum of 7.

NOTE: Configuration of 802.1x Wi-Fi setups is beyond the scope of this deployment guide. Please reference the Intel SCS User Guide for additional detail.

If the client platform has an external switch to enable or disable WLAN, the switch must be in the ON position for Intel AMT over wireless to be configured and to operate. Once enabled, only a full un-provision or un-configuration of the AMT firmware will disable the setting.
9.2.1 PKI DNS Suffix

To remotely configure LAN-less Intel AMT Release 10 systems the correct PKI DNS Suffix for your organization must be defined within the Intel MEBx. This section addresses how to manually add this.

1. During POST enter the Intel MEBX using the appropriate method dependent upon the OEM i.e. <CTRL-P>, F12 etc.

2. If this is the first time the MEBX has been accessed, enter the default Intel ME password (admin). You are forced to ensure you make a note of this.

3. Select Intel AMT Configuration and Remote Setup and Configuration

4. Select TLS PKI and PKI DNS Suffix.

5. Enter the PKI DNS Suffix for your domain. This will be the value supplied by your organization's DHCP server Option 15.

6. Enter the PKI DNS Suffix for your domain. This is the value supplied by your organization's DHCP server Option 15.

7. Press the Esc key to save and exit the MEBX menu.

**NOTE:** When un-configuring Intel AMT systems, do NOT perform a full un-provision as the PKI DNS Suffix value will be deleted.
Discover

Refer to section 3.2 for more detail on performing a discovery of Intel AMT systems capabilities. The command line below can also be used to produce an XML file in the directory it was run from.

```
C:\\Configurator>ACUConfig systemdiscovery /noregistry
```

The output file looks similar to below and the required values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WiredLANExists</td>
<td>For LAN-less systems, this value will be “False”. The value can also be “True” assuming the next values are configured.</td>
</tr>
<tr>
<td>AMTVersion</td>
<td>The version of Intel AMT, this value must be 10.x</td>
</tr>
<tr>
<td>AMTPKIDNSSuffix</td>
<td>The value defined for the PKI DNS Suffix as defined in the Intel MEBX</td>
</tr>
</tbody>
</table>

```xml
<?xml version="1.0" encoding="UTF-8"?>
<SystemDiscovery>
  <Capabilities>
    <IsAMTSupported>True</IsAMTSupported>
    <IsCPLASupported>False</IsCPLASupported>
    <IsAMTKVMSupported>True</IsAMTKVMSupported>
    <IsTLSSupported>True</IsTLSSupported>
    <IsAntiTheftSupported>False</IsAntiTheftSupported>
    <IsWirelessLANSupported>True</IsWirelessLANSupported>
    <WiredLANExists>False</WiredLANExists>
    <IsCCMSupported>True</IsCCMSupported>
    <IsHIPSupported>True</IsHIPSupported>
    <IsKVMEnabedInBIOS>True</IsKVMEnabedInBIOS>
    <IsKVMSupportInBIOS>True</IsKVMSupportInBIOS>
    <IsSOLSupportedInBIOS>True</IsSOLSupportedInBIOS>
    <IsIDERSupportedInBIOS>True</IsIDERSupportedInBIOS>
    <IsAMTEnabledInBIOS>True</IsAMTEnabledInBIOS>
    <IsSOLEnabledInBIOS>True</IsSOLEnabledInBIOS>
    <CRLStoreSize>1424</CRLStoreSize>
    <RootCertificatesMaxSize>2500</RootCertificatesMaxSize>
    <RootCertificatesMaxInstances>4</RootCertificatesMaxInstances>
    <FQDNSuffixMaxEntries>4</FQDNSuffixMaxEntries>
    <FQDNSuffixMaxLength>63</FQDNSuffixMaxLength>
    <CertificateChainMaxSize>4100</CertificateChainMaxSize>
    <SupportedCertificateKeyLengths>1024,2048</SupportedCertificateKeyLengths>
  </Capabilities>
</SystemDiscovery>
```
9.4 Remotely Configuring LAN-less Systems

9.4.1 Create AMT Profile

1. In the Intel SCS Console, create a basic profile specifically for LAN-less systems which will be used to configure the Intel AMT system into Client Control mode.

2. In the Optional Settings window, select the Wi-Fi Connection check box and define a Wi-Fi Setup. Without this remote configuration of Intel AMT will not be possible.

3. To automatically replicate wireless profile settings from the host operating system, select “Enable Synchronization of Intel® AMT with host platform WiFi profiles”.

**NOTE**: Intel AMT Release 6.0 onwards includes a Wireless Profile Synchronization feature which synchronizes wireless profiles within the operating system with Intel AMT. To use this feature Intel® PROSet/Wireless Software must be installed on the operating system. For additional information, refer to the Intel® PROSet/Wireless Software documentation.

4. In the System Settings window, leave the default settings. However when defining the password for the Intel AMT admin user, ensure you select only the option named “Use the following password for all systems” and enter the strong password used when configuring the PKI DNS Suffix setting in the MEBX.
9.4.2 Apply AMT Profile (Host-Based Configuration)

1. Select the “basic” profile and then click **Export to XML** to export the profile to an XML file.

   ![Export to XML](image1)

   **NOTE**: Ensure that you do NOT select the check box named **Put locally configured devices in Admin Control mode**.

   ![Export Profile to XML File](image2)

2. Use the **ConfigAMT** option of the Configurator command to configure the Intel AMT system using the exported XML file.

   ```
   C:\>Configurator>RRConfig /version /output console configant BasicLANLessProfile.xml /CmPassword <password>
   ```

3. When the Intel Management and Security (IMSS) system tray applet dialog appears, configuration of the Intel Management Engine (Intel ME) into Client Control mode is complete. Reboot if required (AMT 10 only)

   ![Intel Management Engine](image3)
9.4.3 Move system to Admin Control mode

1. Now use the `MoveToACM` command of the Configurator to move the system to Admin Control mode. Remember to include the MEBX password:

```
C:\Configurator\IntelConfig\override\override console movetoadm 192.168.11.35 AdminPasswd P@ssw0rd
```

2. After the command has completed successfully, Intel AMT will be configured in Admin Control mode and full access to Intel AMT capabilities can be performed over the WLAN as configured in the profile.

3. Optionally you can now use the `ConfigViaRCSOnly` command of the Configurator to reconfigure the system against existing profiles on the Intel RCS.