

# Intel® Setup and Configuration Software (Intel® SCS)

## Legal Notices and Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at [intel.com](http://intel.com).

Cost reduction scenarios described are intended as examples of how a given Intel- based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

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

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

©Intel Corporation.

# Contents

<b>1</b>	<b>Introduction .....</b>	<b>6</b>
1.1	Intel® Setup and Configuration Software (Intel® SCS) overview .....	7
1.2	Intel® Active Management Technology (Intel® AMT) overview .....	7
<b>2</b>	<b>Prerequisites.....</b>	<b>9</b>
2.1	Client software components.....	9
2.2	Supported operating systems .....	9
2.3	Supported Microsoft SQL Server versions .....	10
2.4	Network access and network ports .....	10
2.5	Domain Name System (DNS) .....	11
2.6	Dynamic Host Configuration Protocol (DHCP).....	11
2.7	Microsoft* Certificate Authority (CA) .....	11
2.8	Microsoft* Active Directory (AD) .....	11
<b>3</b>	<b>Install and Configure Intel® SCS and Console .....</b>	<b>12</b>
<b>4</b>	<b>Intel® AMT Provisioning Certificates .....</b>	<b>18</b>
4.1	Introduction .....	18
4.2	Prerequisites.....	19
4.3	Reference .....	19
4.4	Generate a Certificate Signing Request (CSR) .....	21
4.5	Submit a Certificate Signing Request (CSR) .....	21
4.6	Merge the issued certificate .....	21
4.7	Installing Root and Intermediate certificates .....	22
4.8	Install and validate the certificate .....	22
4.9	Verify and validate remote configuration using PKI .....	24
4.9.1	Create an Intel® AMT profile .....	24
4.9.2	Apply the Intel® AMT profile.....	25
4.10	Verify AMT connectivity .....	26
<b>5</b>	<b>Microsoft Active Directory .....</b>	<b>27</b>
5.1	Introduction .....	27
5.2	Prerequisites.....	27
5.2.1	Create a new OU .....	27
5.2.2	Create new AD groups.....	28
5.2.3	Assign permissions to the new OU .....	28
5.3	Verify and validate Microsoft* Directory Integration .....	29
5.3.1	Create an Intel® AMT profile .....	29
5.3.2	Apply the Intel® AMT profile.....	30

5.3.3	Verify Intel® AMT connectivity .....	31
<b>6</b>	<b>Encrypting Communications Using Transport Layer Security (TLS) .....</b>	<b>32</b>
6.1	Introduction .....	32
6.2	Prerequisites.....	32
6.2.1	Request handling.....	33
6.2.2	Create Certificate Template .....	33
6.2.3	Configure the certificate template.....	35
6.2.4	Assign permissions to the certificate template .....	36
6.2.5	Issue certificate template.....	37
6.3	Verify and validate the Transport Layer Security (TLS) configuration .....	39
6.3.1	Create an Intel® AMT profile .....	39
6.3.2	Apply the Intel® AMT profile.....	40
6.3.3	Verify Intel® AMT connectivity .....	40
<b>7</b>	<b>Wireless .....</b>	<b>41</b>
7.1	Introduction .....	41
7.2	Prerequisites.....	41
7.2.1	PKI DNS Suffix .....	41
7.3	Discover .....	43
7.4	Remotely configuring LAN-less systems .....	43
7.4.1	Create an Intel® AMTprofile .....	43
7.4.2	Apply Intel® AMT profile (Host-based configuration) .....	44
7.4.3	Move system to Admin Control mode .....	46
<b>8</b>	<b>Configuration .....</b>	<b>47</b>
8.1	Introduction .....	47
8.2	Configuration methods .....	47
8.3	Remote configuration using PKI .....	48
8.4	Host-based configuration .....	49
8.5	Using the Intel® AMT Configuration Utility Wizard .....	49
8.6	Using the Intel® AMT Configuration Utility Command Line Interface (CLI) .....	51
8.7	Manual configuration .....	52
8.8	Manual configuration (multiple systems) .....	54
8.9	Unconfigure method .....	54
<b>9</b>	<b>Discovery .....</b>	<b>57</b>
9.1	Introduction .....	57
9.2	Using the configurator .....	57
9.3	Using the SCS_Discovery utility .....	59
9.4	Using the RCS.....	60

9.5 Using the Platform Discovery utility .....60

9.6 Using the Solutions Framework.....60

## Revision History

Revision	Revision History	Date
1.0	Initial release	July 2015
1.1	Updates for Intel® SCS 12.0	January 2019

# 1 Introduction

This deployment guide is an instructional document providing simple steps to enable the discovery, configuration and maintenance 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<sup>1</sup>.

Guidance is provided to enable a baseline implementation of Intel® AMT and identifies common configuration settings to support an enterprise deployment that take advantage of the manageability and security features available on platforms that support Intel® AMT and Intel® Standard Manageability<sup>2</sup>

After configuration, Intel® AMT systems can be remotely managed by products, toolsets and solutions including Microsoft System Center Configuration Manager\*, Microsoft PowerShell\*, and Intel® Manageability Commander.

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

- Utilizing hardware based KVM Remote Control to reduce maintenance and support costs and avoid desk-side visits<sup>3</sup>.
- Improving system deployment and rebuild processes.
- Keeping clients updated and avoid working hour reboots, even for remote employees.
- Providing effective remote assistance whilst outside the corporate network.
- Providing an effective decommission process for retired machines.

The guide compliments the Intel® Setup and Configuration Software (Intel® SCS) User Guide (*Intel(R)\_SCS\_User\_Guide.pdf*) in the Intel® SCS download package that is available from <http://www.intel.com/go/scs>.

---

<sup>1</sup> Intel® Active Management Technology features may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, or on battery power when in a low power state or powered off. For more information, visit [intel.com/AMT](http://intel.com/AMT).

<sup>2</sup> Intel® Standard Manageability (ISM) systems were introduced with Intel® AMT Release 5.0 and have a subset of Intel® AMT features e.g. no KVM, Wireless LAN support, etc.

<sup>3</sup> KVM (Keyboard, Video, and Mouse) Remote Control is only available with Intel® Core™ vPro™ processors with active integrated graphics. Discrete graphics are not supported.

## 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:

- A 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™ 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.

Intel® SCS includes the components listed below. However, only some of these components are used or referenced within this guide. Please see 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 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 that can be used to configure multiple Intel® AMT systems.
- **Discovery Utility:** SCSDiscovery.exe is a standalone utility used to gather detailed information about Intel® AMT.
- **Remote Configuration Service Utility:** RCSUtils.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™ Platforms. Intel® AMT is also available on select IoT and Workstation devices.

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 Intel® 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 either available via a system BIOS menu or can be displayed if you press a special key combination, traditionally <Ctrl-P>, during the system boot process.
- The Intel® Management Engine Interface<sup>4</sup> (Intel® MEI) driver, is the operating software interface to the Intel® AMT device.
- The Intel® Local Manageability Service<sup>56</sup> (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.

---

<sup>4</sup> The MEI driver and LMS are 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.

<sup>5</sup> The LMS is installed on a platform that has Intel® AMT Release 9.0 or greater.

<sup>6</sup> 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® SCS User Guide, available in the Intel® SCS download package.

**Note:** Depending on 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® ME 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 Intel Management Engine Interface (Intel® 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

Table 2–1 describes which operating systems the main Intel® SCS components can run on.

**Table 2–1** Supported operating systems

Version	Configurator	RCS	Console
Windows* 10 Pro	Yes	No	No
Windows 10 Enterprise	Yes	No	No
Windows 8.1 Pro	Yes	No	No
Windows 8.1 Enterprise	Yes	No	No
Windows 7 Professional (SP1)	Yes	Yes	Yes
Windows 7 Enterprise (SP1)	Yes	Yes	Yes
Windows Server* 2016	No	Yes	Yes
Windows Server 2012 R2	No	Yes	Yes
Windows Server 2012	No	Yes	Yes
Windows Server 2008 R2 (SP2)	No	Yes	Yes
Windows Server 2008 (SP2)	No	Yes	Yes
* 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 now supports the Standard and Enterprise editions of Microsoft SQL Server as listed in Table 2–2..

**Table 2–2 Supported Microsoft SQL Server versions**

Version	Enterprise	Standard
Microsoft SQL Server 2016	Yes	Yes
Microsoft* SQL Server* 2014	Yes	Yes
Microsoft SQL Server 2012	Yes	Yes
Microsoft SQL Server 2008 R2 (SP1 and higher)	Yes	No
Microsoft SQL Server 2008 (SP1 and higher)	Yes	No
* Other names and brands may be claimed as the property of others.		

## 2.4 Network access and network ports

Intel® SCS can enable Intel® AMT different configurations. Intel® AMT Releases 2.5, 2.6, 4.0, 6.0 and later support a wireless and wired network interface. Table 2–3 provides a summary of the ports and protocols that can be used.

**Table 2–3 Network access and network ports**

Port	Description	Details
53	DNS	Intel® SCS and Intel® AMT will use DNS to identify clients.
88	Kerberos	Intel® SCS and Intel® AMT will use Kerberos to authenticate SCS service account and users
135	RPC	Intel® SCS and Intel® AMT will leverage DCOM to initiate connections
389 / 636	LDAP/LDAP over TLS/SSL	Intel® SCS and Intel® AMT will interact with Microsoft Active Directory
3268	Microsoft Global Catalog	Intel® SCS will search Microsoft Global Catalog for user, groups, and computers
49152 – 65335	Dynamic Port Range	Intel® SCS and Intel® AMT will leverage dynamic ports unless static ports have been identified for various services
16992	Intel(R) AMT HTTP	Used for WS-Management messages to and from Intel® AMT.
16993	Intel(R) AMT HTTPS	Used for WS-Management messages to and from Intel® AMT when TLS is enabled.
16994	Intel(R) AMT Redirection/TCP	Used for redirection traffic (SOL, IDER, and KVM using Intel® AMT authentication).
16995	Intel(R) AMT Redirection/TLS	Used for redirection traffic (SOL, IDER, and KVM using Intel® AMT authentication) when TLS is enabled.
623	ASF Remote Management and Control Protocol (ASF-RMCP)	Used for RMCP pings. This port is a standard DMTF port and accepts WS-Management traffic. It is always enabled.
664	DMTF out-of-band encrypted web services management protocol ASF Remote Management and Control Protocol (ASF-RMCP)	Used for encrypted RMCP pings. This port is always enabled and is a standard DMTF port that accepts encrypted WS-Management traffic.
5900	VNC (Virtual Network Computing) – remote control program	Used for KVM viewers that do not use Intel® AMT authentication but use the standard VNC port instead .

**Note:** Depending on the configuration path chosen, the infrastructure components described in the following sections 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 Encrypting 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 be performed by an Enterprise CA or a Standalone CA.

## 2.8 Microsoft\* Active Directory (AD)

Intel® SCS 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 Install and Configure Intel® SCS and Console

As discussed in Section 1.1 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 server in the network.

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

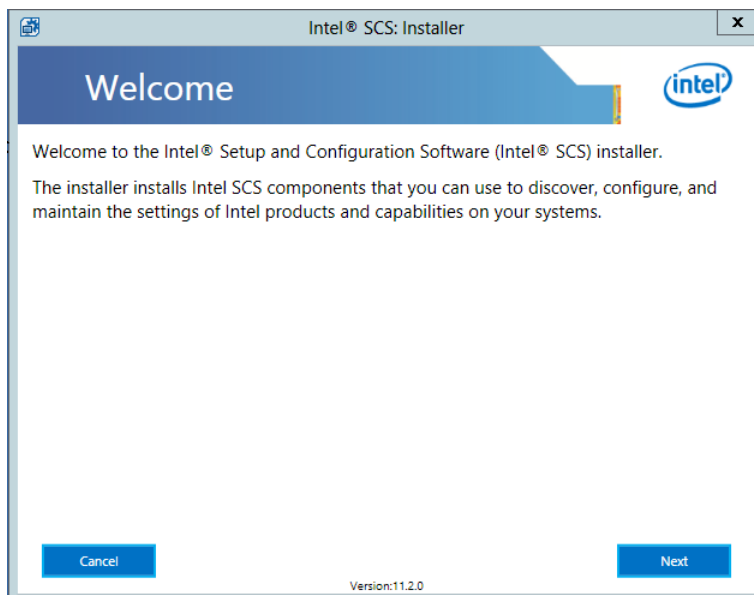
- Place Intel® AMT devices into Admin Control Mode (ACM)
- Use the Remote Configuration approach
- Use the One-Touch Configuration approach
- Use Digest Master Passwords

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)

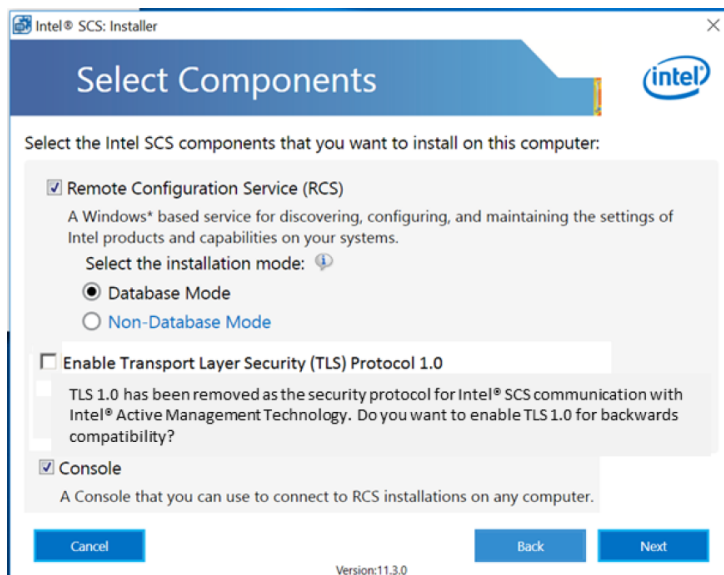
For the purposes of this guide, Intel® SCS will be installed in Database Mode with the Remote Configuration Service (RCS) and console installed locally. In this mode, the RCS does not store data about the Intel® AMT systems. Configuration and maintenance tasks can only be done using the Configurator. 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 panel of the Intel® SCS Installer window appears. Click the **Next** button.



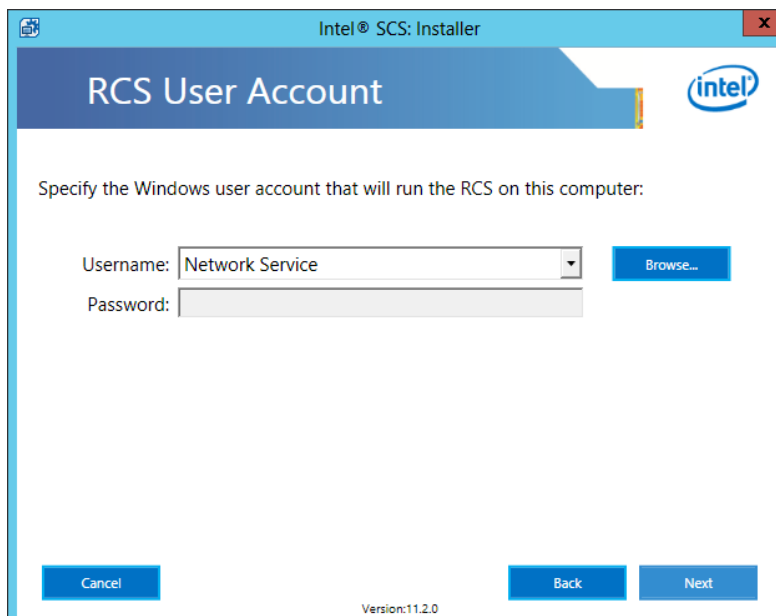
2. Select **I accept the terms of the license agreement** and click the **Next** button. The Select Components panel appears.

3. Ensure the **Remote Configuration Service (RCS)** and **Console** are selected. The **Database Mode** setting is *Default* and for this guide the **Database Mode** option is *selected*.



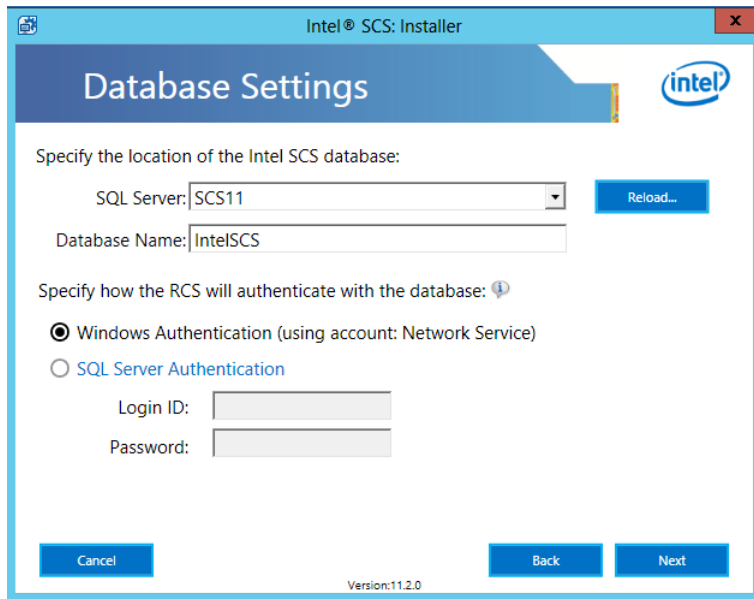
**Note:** Intel® SCS 12.0 defaults to TLS 1.1 to encrypt communication to Intel® AMT. TLS 1.0 has been deprecated as the security protocol for Intel® SCS communication with Intel® AMT, as the TLS 1.0 protocol has identified security vulnerabilities, including CVE-2011-3389 and CVE-2014-3566. Intel® SCS allows users to enable TLS 1.0 protocol support for backwards compatibility with legacy Intel® AMT platforms. For this example we have left TLS 1.0 support disabled. Please reference the *Intel® SCS User Guide* for additional details.

4. Click the **Next** button.
5. The Windows operating system includes a built-in security account named “Network Service.” This account increases security as its not easy to impersonate a computer. 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.



6. Select or enter the SQL Server name. The database name is created by default.

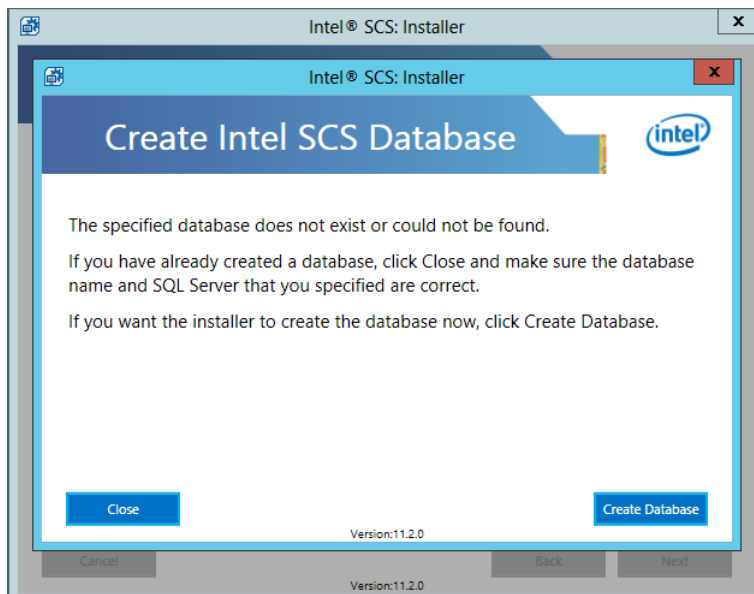
**Note:** The account used to log into SQL Server must have the **dbcreator** and **securityadmin** Server Roles in SQL Server.



The screenshot shows the 'Database Settings' window of the Intel SCS Installer. The window title is 'Intel® SCS: Installer'. The main heading is 'Database Settings'. Below the heading, there is a section 'Specify the location of the Intel SCS database:'. It contains a 'SQL Server:' dropdown menu with 'SCS11' selected, a 'Database Name:' text box with 'IntelSCS', and a 'Reload...' button. Below this is a section 'Specify how the RCS will authenticate with the database:'. It has two radio buttons: 'Windows Authentication (using account: Network Service)' which is selected, and 'SQL Server Authentication'. Under 'SQL Server Authentication', there are 'Login ID:' and 'Password:' text boxes. At the bottom, there are 'Cancel', 'Back', and 'Next' buttons. The version 'Version:11.2.0' is displayed at the bottom center.

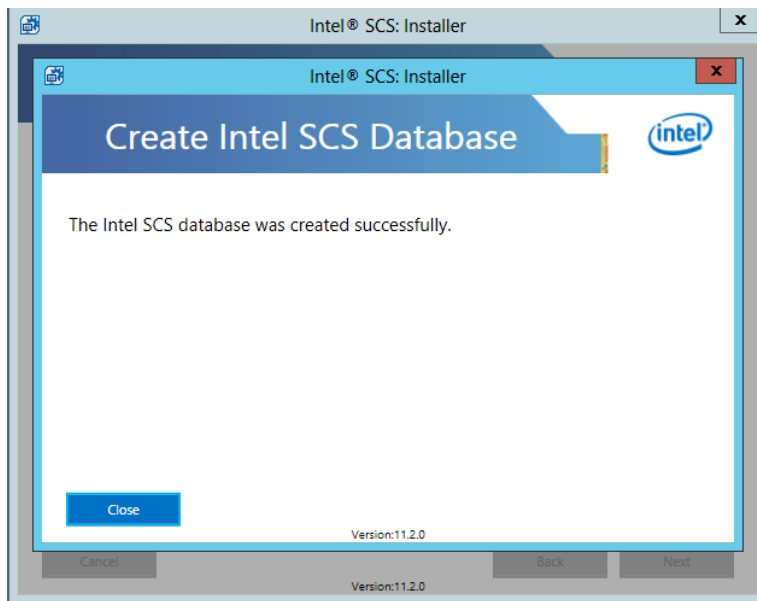
Click **Next** and the installer will test the SQL connection.

7. The installer will detect if there is an Intel® SCS database present. In this example, there isn't one installed and the installer will create the database. Select **Create Database** to continue.

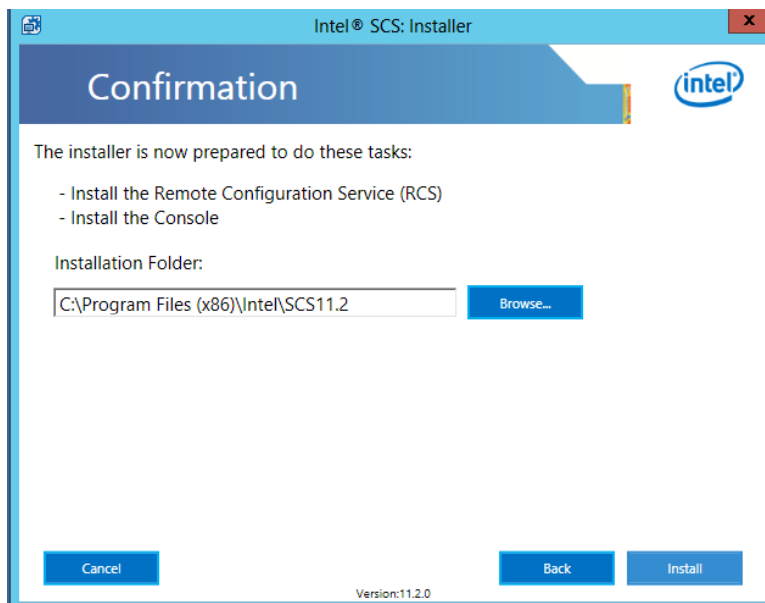


The screenshot shows the 'Create Intel SCS Database' window of the Intel SCS Installer. The window title is 'Intel® SCS: Installer'. The main heading is 'Create Intel SCS Database'. Below the heading, there is a message: 'The specified database does not exist or could not be found. If you have already created a database, click Close and make sure the database name and SQL Server that you specified are correct. If you want the installer to create the database now, click Create Database.' At the bottom, there are 'Close' and 'Create Database' buttons. The version 'Version:11.2.0' is displayed at the bottom center.

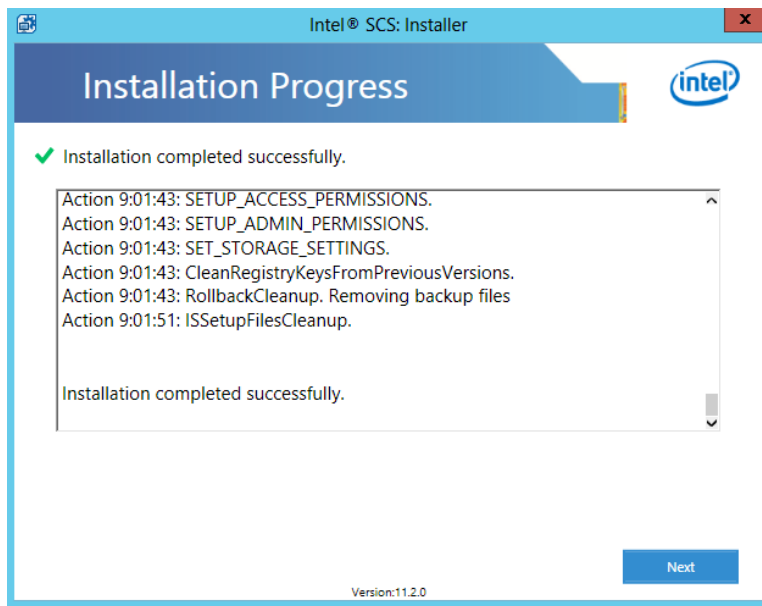
8. The installer will return successfully. Select **Close** to continue the installation.



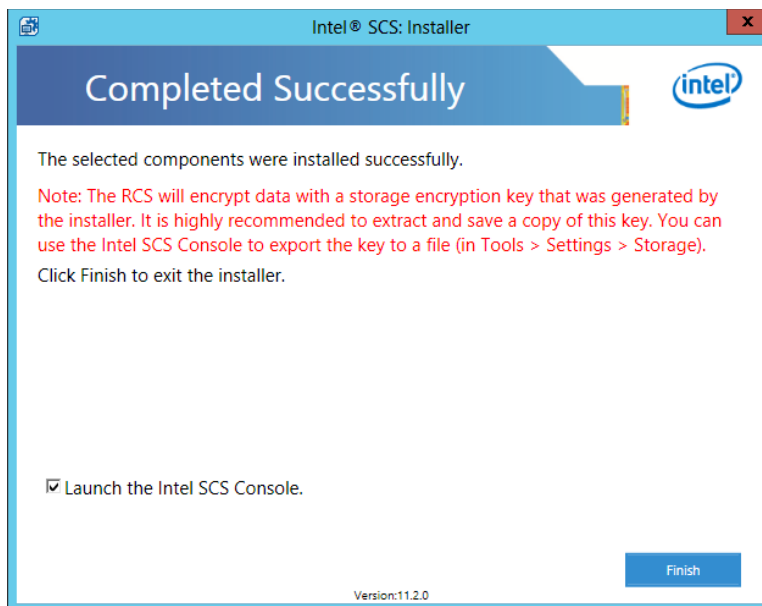
9. Click the **Next** button. The Confirmation panel appears, showing information about the selections made. The default installation folder is **C:\Program Files(x86)\Intel\SCS12**. If you want to change the location, type a new path in the Installation Folder field or click the **Browse** button to select one.



10. Click the **Install** button. The Installation Progress panel appears. When installation is complete, a message announces it.



11. Click the **Next** button. The Completed Successfully panel appears.

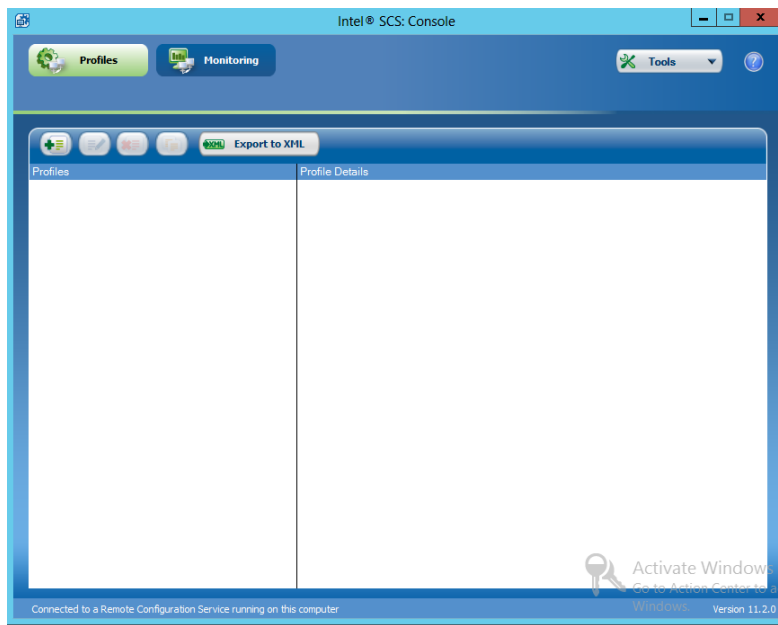


12. Click the **Finish** button. The installer window closes.

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*).



The Intel® SCS Console appears if you left **Launch the Intel® SCS Console** check box selected.



## 4 Intel® AMT Provisioning Certificates

### 4.1 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 RCS and Intel® AMT systems when initiating client configuration into Admin Control Mode.

Dependent upon Intel® AMT Release, the firmware contains root certificate hashes from a number of commercial Certificate Authorities including GoDaddy\*, Comodo\*, and Entrust\*. From Intel® AMT Release 7.0, you can add your own root certificate hashes into the Intel® MEBX (up to 10 custom SHA1 hashes). Additional details on supported Root Certificate Hashes is available in the *Intel® AMT Implementation and Reference Guide* at [https://software.intel.com/sites/manageability/AMT\\_Implementation\\_and\\_Reference\\_Guide/WordDocuments/rootcertificatehashes.htm](https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/WordDocuments/rootcertificatehashes.htm)

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 Manual Configuration do not require an AMT provisioning certificate and HBC remains the recommended option, if mandatory user consent requirement for redirection operations is acceptable.

This section provides simple, step-by-step instructions to obtain an Intel® AMT provisioning certificate suitable for use with remote configuration of Intel® AMT systems using freely available OpenSSL tools.

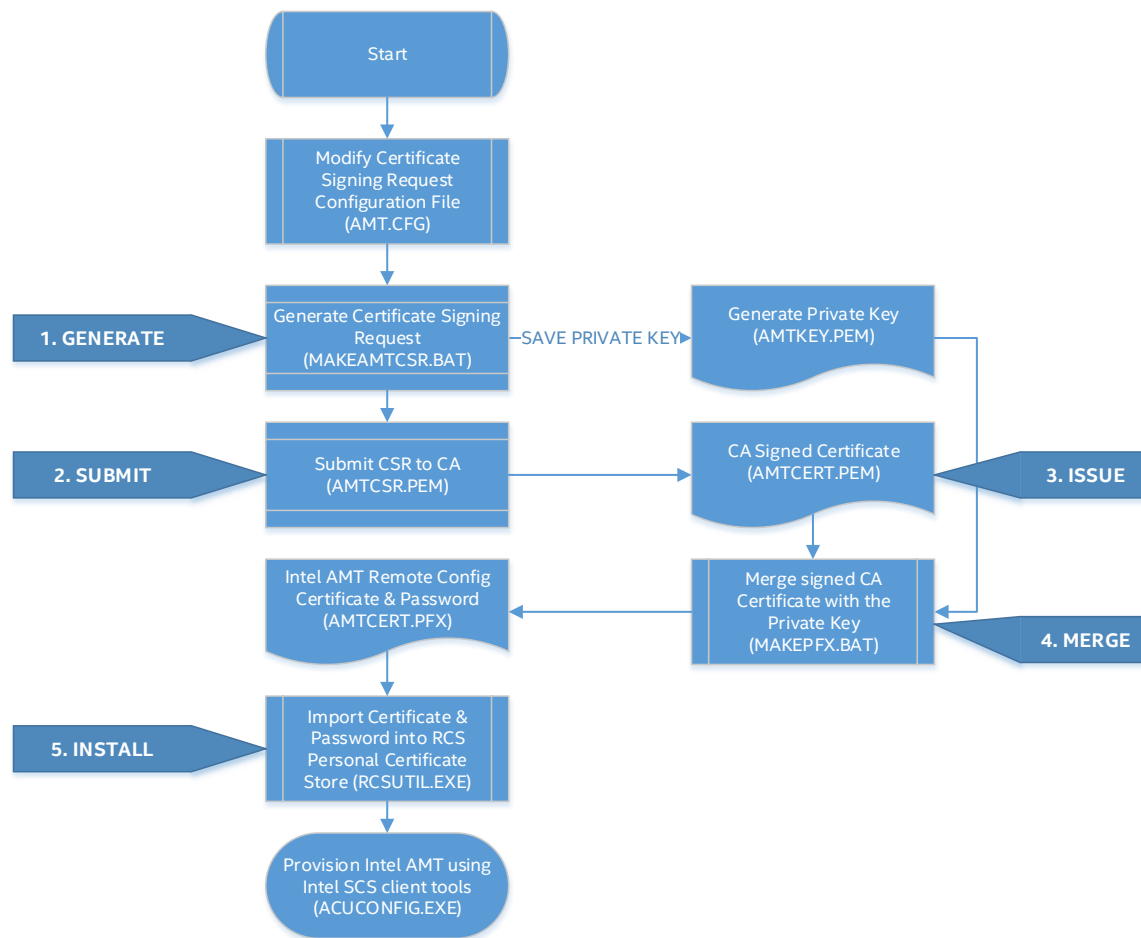
Figure 4-1 illustrates the necessary steps and overall flow to support this process, which consists of the following five high-level steps:

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."

**Figure 4-1 Intel® AMT provisioning flow**



Alternative guides are available on how to purchase and install certificates below. For more information, please go to our [Intel Active Management Technology Implementation website](#).

## 4.2 Prerequisites

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

**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.

## 4.3 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

## 4.4 Generate a 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 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, site, 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**  
**Note:** None of the fields in **[ req\_extensions\_section ]** section should be changed unless requesting a Unified Communication Certificate (UCC), in which case uncomment the **'subjectAltName'** field.
4. Save the edited **AMT.CFG** file.
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 that you safely store and backup the private key **AMTKEY.PEM** and the CSR file **AMTCSR.PEM** created in step 5.

## 4.5 Submit a 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**.

## 4.6 Merge the 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 it into RCS's Local Machine certificate store. To carry out this process follow these instructions:

1. 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---'**.
2. Ensure **AMTCERT.PEM** is in the same directory as the private key **AMTKEY.PEM**.

3. 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.

## 4.7 Installing Root and Intermediate certificates

The Intel® 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 (**RCSSTServer.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.

## 4.8 Install and validate the certificate

This guide uses the Network Service account to run the RCS and the Intel® 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*.

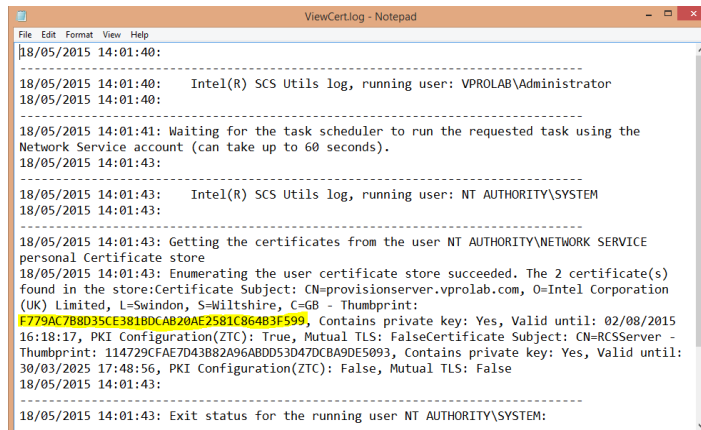
**Note:** For systems running Microsoft Windows 7\* or newer operating systems, this executable must be opened with elevated privileges due to interaction with a kernel level driver. This is done by right-clicking on the executable and selecting **Run as administrator**.

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**

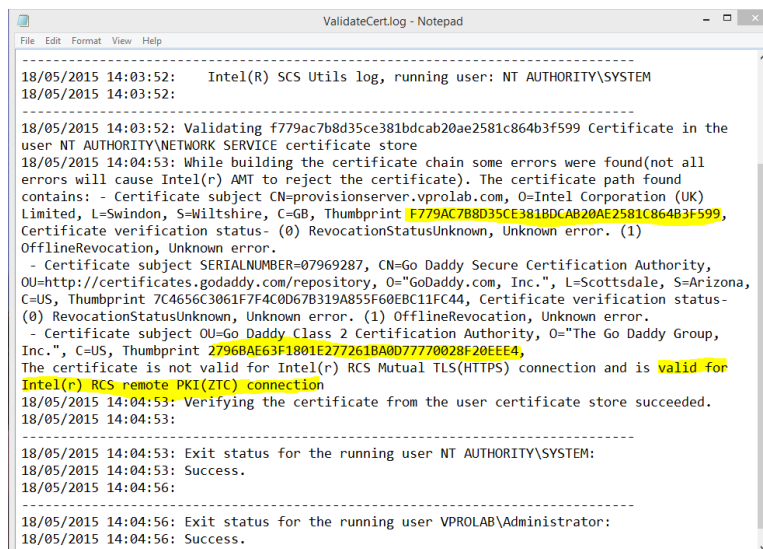


```
ViewCert.log - Notepad
File Edit Format View Help
18/05/2015 14:01:40:
-----
18/05/2015 14:01:40: Intel(R) SCS Utils log, running user: VPROLAB\Administrator
18/05/2015 14:01:40:
-----
18/05/2015 14:01:41: Waiting for the task scheduler to run the requested task using the
Network Service account (can take up to 60 seconds).
18/05/2015 14:01:43:
-----
18/05/2015 14:01:43: Intel(R) SCS Utils log, running user: NT AUTHORITY\SYSTEM
18/05/2015 14:01:43:
-----
18/05/2015 14:01:43: Getting the certificates from the user NT AUTHORITY\NETWORK SERVICE
personal Certificate store
18/05/2015 14:01:43: Enumerating the user certificate store succeeded. The 2 certificate(s)
found in the store:Certificate Subject: CN=provisionserver.vprolab.com, O=Intel Corporation
(UK) Limited, L=Swindon, S=Wiltshire, C=GB - Thumbprint:
F779AC7B8D35CE381BDCAB20AE2581C864B3F599, Contains private key: Yes, Valid until: 02/08/2015
16:18:17, PKI Configuration(ZTC): True, Mutual TLS: FalseCertificate Subject: CN=RCSUser -
Thumbprint: 114729CFAE7D43B82A96ABDD53D47DCBA9DE5093, Contains private key: Yes, Valid until:
30/03/2025 17:48:56, PKI Configuration(ZTC): False, Mutual TLS: False
18/05/2015 14:01:43:
-----
18/05/2015 14:01:43: Exit status for the running user NT AUTHORITY\SYSTEM:
```

**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.

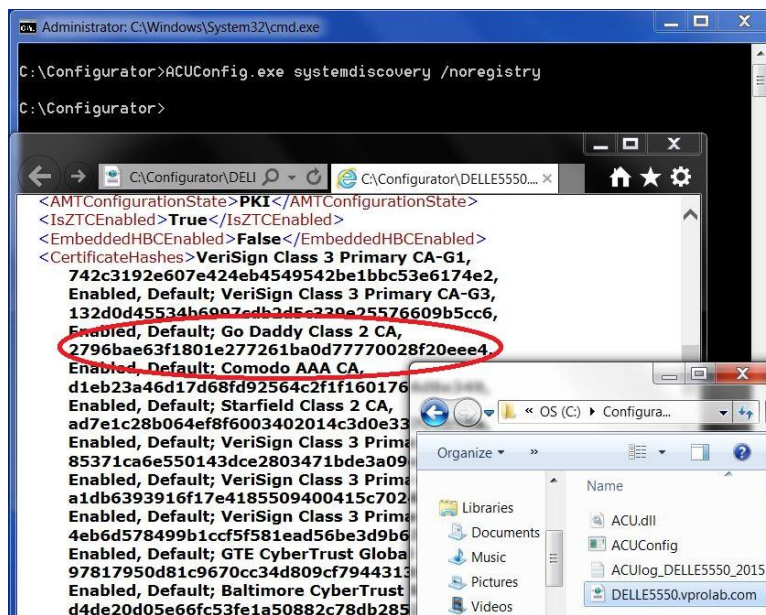
You will see your AMT Provisioning Certificate with its thumbprint (hash) listed. This is required to validate the certificate and signing chain for remote configuration in the step below.

**RCSUtils.exe /Certificate Validate F779AC7B8D35CE381BDCAB20AE2581C864B3F599 /RCSUser NetworkService /Log File ValidateCert.log**



```
ValidateCert.log - Notepad
File Edit Format View Help
18/05/2015 14:03:52: Intel(R) SCS Utils log, running user: NT AUTHORITY\SYSTEM
18/05/2015 14:03:52:
-----
18/05/2015 14:03:52: Validating f779ac7b8d35ce381bdcab20ae2581c864b3f599 Certificate in the
user NT AUTHORITY\NETWORK SERVICE certificate store
18/05/2015 14:04:53: While building the certificate chain some errors were found(not all
errors will cause Intel(r) AMT to reject the certificate). The certificate path found
contains: - Certificate subject CN=provisionserver.vprolab.com, O=Intel Corporation (UK)
Limited, L=Swindon, S=Wiltshire, C=GB, Thumbprint F779AC7B8D35CE381BDCAB20AE2581C864B3F599,
Certificate verification status- (0) RevocationStatusUnknown, Unknown error. (1)
OfflineRevocation, Unknown error.
- Certificate subject SERIALNUMBER=07969287, CN=Go Daddy Secure Certification Authority,
OU=http://certificates.godaddy.com/repository, O="GoDaddy.com, Inc.", L=Scottsdale, S=Arizona,
C=US, Thumbprint 7C4656C3061F7F4C0D67B319A855F60EBC11FC44, Certificate verification status-
(0) RevocationStatusUnknown, Unknown error. (1) OfflineRevocation, Unknown error.
- Certificate subject OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group,
Inc.", C=US, Thumbprint 27968AE63F1801E277261BA007770028F20EEE4,
The certificate is not valid for Intel(r) RCS Mutual TLS(HTTPS) connection and is valid for
Intel(r) RCS remote PKI(ZTC) connection
18/05/2015 14:04:53: Verifying the certificate from the user certificate store succeeded.
18/05/2015 14:04:53:
-----
18/05/2015 14:04:53: Exit status for the running user NT AUTHORITY\SYSTEM:
18/05/2015 14:04:53: Success.
18/05/2015 14:04:56:
-----
18/05/2015 14:04:56: Exit status for the running user VPROLAB\Administrator:
18/05/2015 14:04:56: Success.
```

View the resulting log file identifies the complete certificate chain and provides a message that the certificate is valid for Intel RCS Remote PKI.



## 4.9 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).

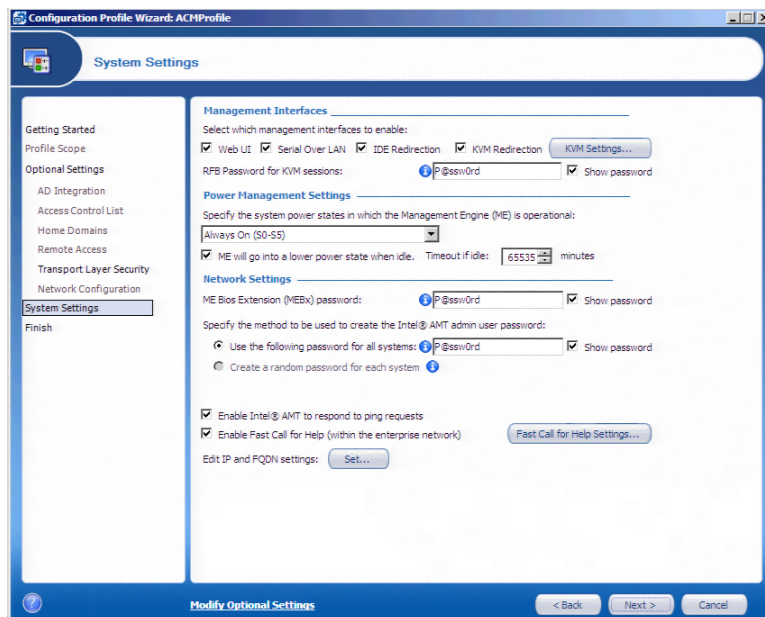
This presents problems for some of the latest Intel vPro™ Platforms that do not include an onboard wired LAN interface, only a wireless interface.

Intel® AMT Release 9.x systems cannot be configured entirely remotely, however Intel® AMT Release 10.x and newer systems fully support remote configuration. The configuration of these LAN-less Platforms is covered in the Wireless section.

### 4.9.1 Create an Intel® 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
  - **Intel® MEBX Password:** P@ssw0rd
  - **Intel® AMT Admin Password:** P@ssw0rd
  - **Enable Intel® AMT** to respond to ping requests

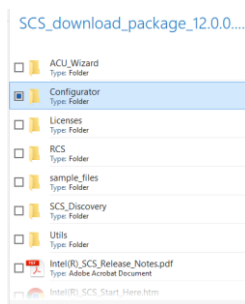




- Click the **OK**, **Next**, and **Finish** buttons to complete the profile.

## 4.9.2 Apply the Intel® AMT profile

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

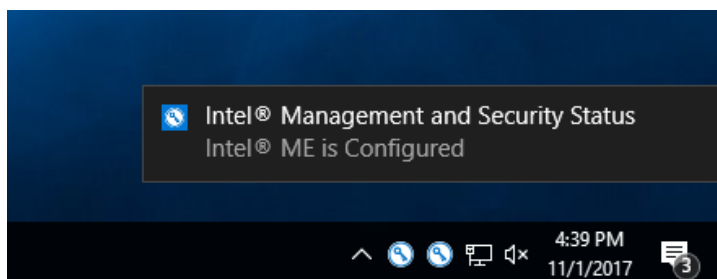


- Open a command prompt on the Intel® AMT system, using *Run as Administrator* and change to the Configurator directory.
- Run the following command:

**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*.

- When the Intel Management and Security (IMSS) toast notification appears, the Intel Management Engine (Intel® ME) configuration is complete.

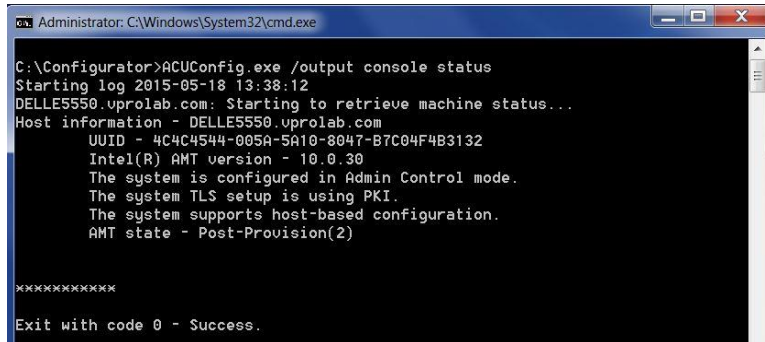


## 4.10 Verify AMT connectivity

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**

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



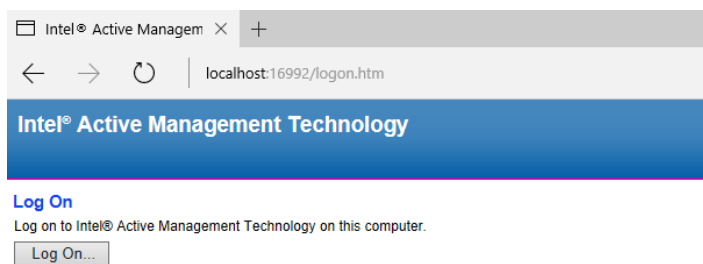
```
Administrator: C:\Windows\System32\cmd.exe
C:\Configurator>ACUConfig.exe /output console status
Starting log 2015-05-18 13:38:12
DELLE5550.uprolab.com: Starting to retrieve machine status...
Host information - DELLE5550.uprolab.com
  UUID - 4C4C4544-005A-5A10-8047-B7C04F4B3132
  Intel(R) AMT version - 10.0.30
  The system is configured in Admin Control mode.
  The system TLS setup is using PKI.
  The system supports host-based configuration.
  AMT state - Post-Provision(2)

*****
Exit with code 0 - Success.
```

2. From the SCS console system, open a web browser and enter the URL for the Intel® AMT System: <http://FQDN:16992>

If the Intel® Active Management Technology webpage appears, the managed client is configured.

3. Click the **Log On** button.



4. Enter the default user "admin" and the password set using the profile: P@ssw0rd.

## 5 Microsoft Active Directory

### 5.1 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 Kerberos with 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. For more information refer to the *Intel® SCS User 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 unconfiguration 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, as shown in Table 5–1.

**Table 5–1** Service Principal Names (SPNs)

SPN	Service
HTTP/FQDN:16992	SOAP over HTTP
HTTP/FQDN:16993	SOAP over HTTPS
HTTP/FQDN:16994	Redirection over TCP
HTTP/FQDN:16995	Redirection over TLS
HTTP/FQDN:623	DMTF manageability over TCP
HTTP/FQDN:664	DMTF manageability over TLS

**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.

### 5.2 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.”

#### 5.2.1 Create a new OU

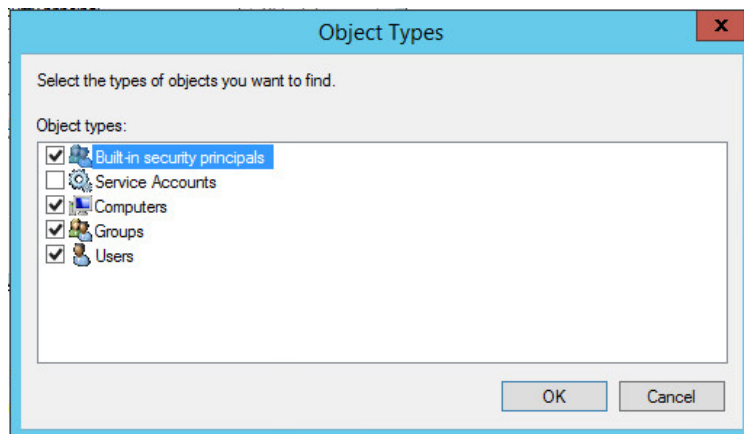
To separate the two Computer objects, it is best practice to create a separate Active Directory Organization Unit (OU) to store Intel® AMT Computer objects (For example: **AMT\_OU**). Control of this OU must be assigned

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.

## 5.2.2 Create new AD groups

It is highly recommended that several AD Domain groups are created with suitable permissions to access common Intel® AMT features. Roles such as Administrators, Support Engineers, Service or Help Desk should have permissions assigned based upon the requirements of a 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 AD group members including “Domain Admin”, “Domain Computers” and the Computer object representing the Network Service account running the RCS with the access type set to “Both.” To add the Computer object this you must select the object type to “Computers.”



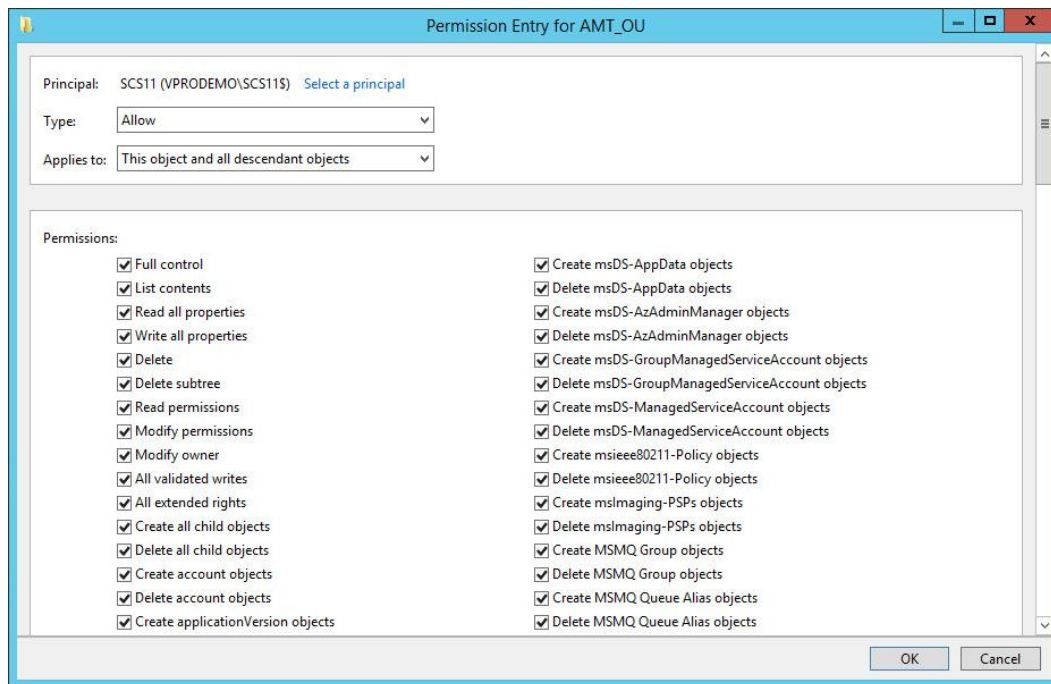
**Service Desk:** Access is limited to the following Realms over both interfaces to support the majority of standard Intel® AMT use cases:

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

## 5.2.3 Assign permissions to the new OU

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

**This object and all descendant Objects only: Full Control.**

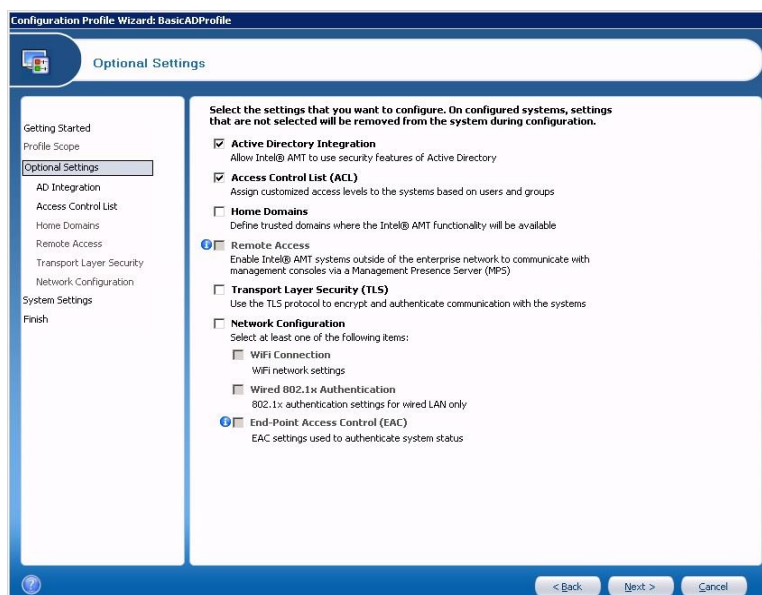


## 5.3 Verify and validate Microsoft\* Directory Integration

### 5.3.1 Create an Intel® AMT profile

Follow the steps as defined in the **Install and Validate the Certificate** section to create a new profile, named BasicADProfile.

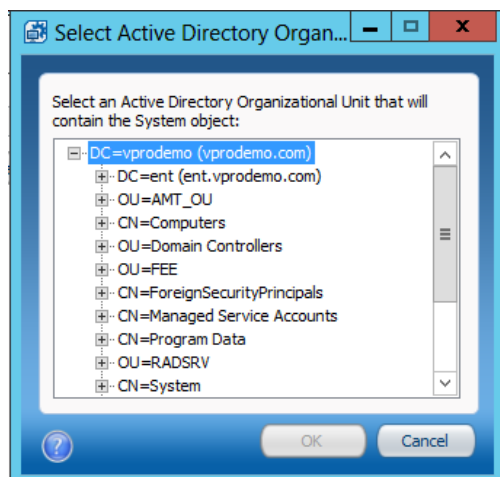
1. In the Getting Started window, select **Configuration/Reconfiguration**.
2. Click the **Next** button and select the **Optional Settings** window with the following options:
  - **Active Directory Integration**
  - **Access Control List (ACL)**



**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. Digest User can only be used for authentication.

In the Active Directory OU box, locate the **AMT\_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 Administrators** 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 Administrators** 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.



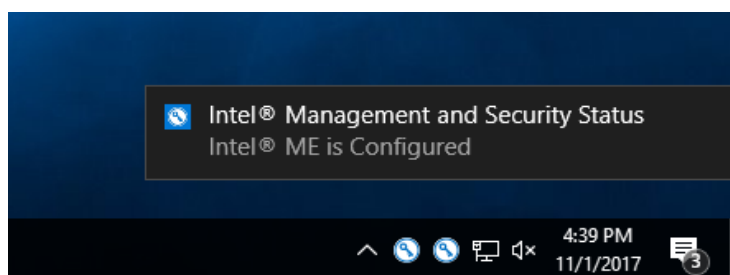
### 5.3.2 Apply the Intel® AMT profile

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:

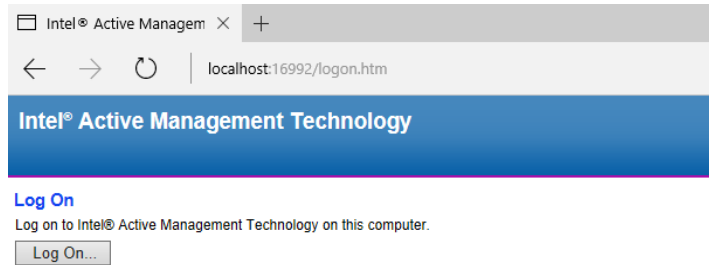
**ACUConfig.exe ConfigAMT BasicADProfile.xml /DecryptionPassword P@ssword**



### 5.3.3 Verify Intel® 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® Active Management Technology webpage displays, the managed client is configured.



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 may be required to enable Kerberos authentication over non-standard HTTP ports such as 16992/16993.

## 6 Encrypting Communications Using Transport Layer Security (TLS)

### 6.1 Introduction

Transport Layer Security (TLS) is an optional feature that helps secure 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 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.”

### 6.2 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:

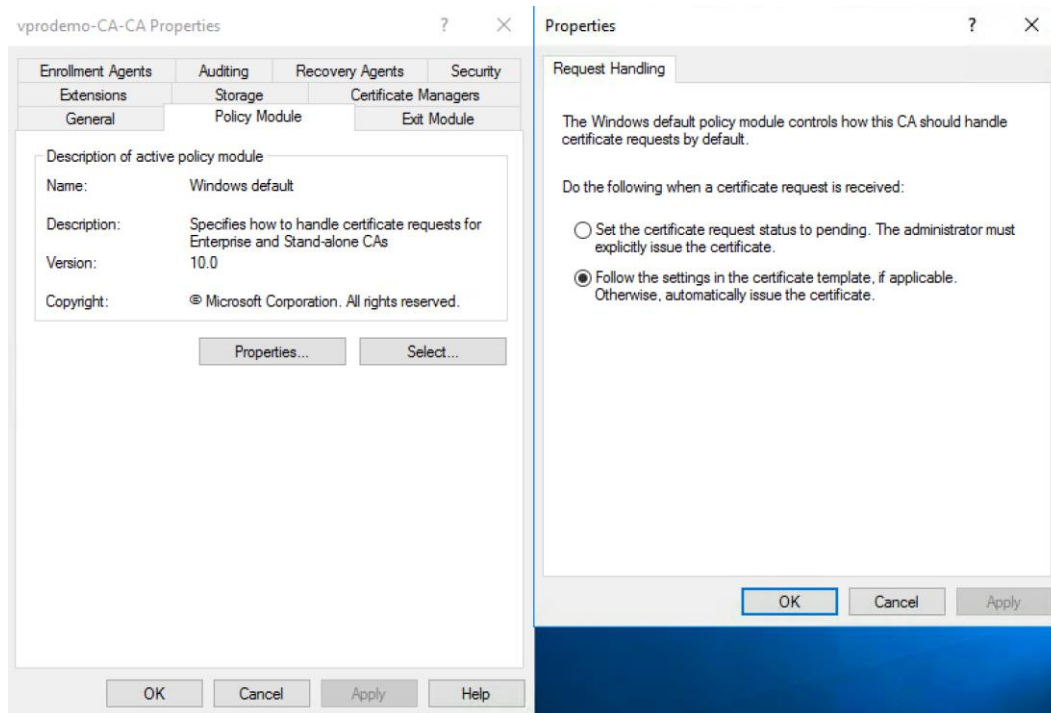
- Issue and Manage Certificates
- Request Certificates
- Read Certificates
- Enroll Certificates

Within this deployment guide, the account used is the SCS server computer account (ex: SCS\$).



## 6.2.1 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.



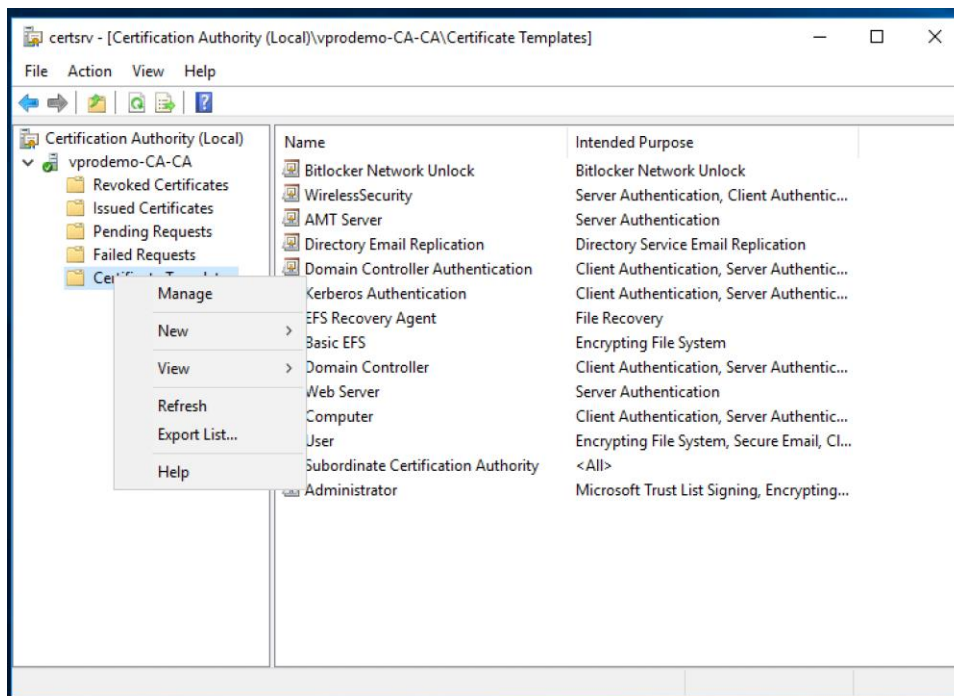
## 6.2.2 Create Certificate Template

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.

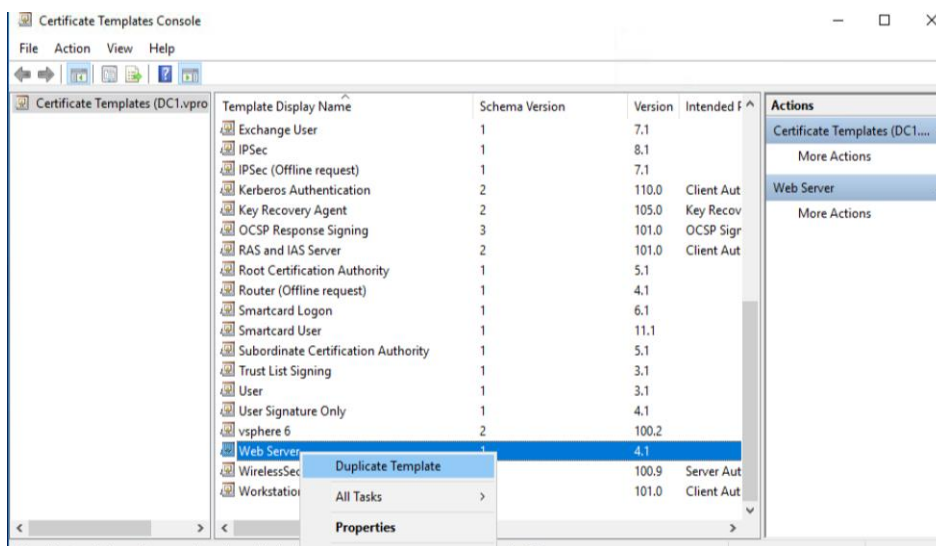
**Note:** Certificate Revocation Lists (CRL) are not covered in this section and Intel RCS does not use the original CRL file supplied by the Certification Authority. Additionally CRL is only available to Intel® AMT when you configure mutual TLS authentication which is beyond the scope of this deployment guide. For additional detail refer to the *Intel® SCS User Guide* section “Preparing the Certification Authority.”

1. From your Certificate Authority, run the Microsoft Management Console with the Certificate Templates plug-in.

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



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



- 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.

### 6.2.3 Configure the 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.

The screenshot shows the 'Properties of New Template' dialog box with the 'General' tab selected. The 'Template display name' field contains 'Copy of Web Server'. The 'Template name' field also contains 'Copy of Web Server'. The 'Validity period' is set to '2 years' and the 'Renewal period' is set to '6 weeks'. The 'Publish certificate in Active Directory' checkbox is unchecked. Below it, the checkbox 'Do not automatically reenroll if a duplicate certificate exists in Active Directory' is also unchecked. At the bottom, there are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

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.

The screenshot shows the 'Properties of New Template' dialog box with the 'Request Handling' tab selected. The 'Purpose' dropdown is set to 'Signature and encryption'. The checkbox 'Delete revoked or expired certificates (do not archive)' is unchecked. The checkbox 'Include symmetric algorithms allowed by the subject' is checked. The checkbox 'Archive subject's encryption private key' is unchecked. The checkbox 'Authorize additional service accounts to access the private key (\*)' is unchecked, with a 'Key Permissions...' button next to it. The checkbox 'Allow private key to be exported' is checked. The checkbox 'Renew with the same key (\*)' is unchecked. The checkbox 'For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (\*)' is unchecked. Under the section 'Do the following when the subject is enrolled and when the private key associated with this certificate is used:', the radio button 'Enroll subject without requiring any user input' is selected. The other two radio buttons are unselected. At the bottom, there are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

- Click the **Cryptography** tab, and in the list of requests, select the **Microsoft Strong Cryptographic Provider and Microsoft Enhanced Cryptographic Provider v1.0** check box, and click the **OK** button.

Properties of New Template

Subject Name    Server    Issuance Requirements

Superseded Templates    Extensions    Security

Compatibility    General    Request Handling    **Cryptography**    Key Attestation

Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

☐ Requests can use any provider available on the subject's computer

☒ Requests must use one of the following providers:

Providers:

- ☒ Microsoft Strong Cryptographic Provider
- ☒ Microsoft RSA SChannel Cryptographic Provider
- ☒ Microsoft DH SChannel Cryptographic Provider
- ☒ Microsoft Enhanced Cryptographic Provider v1.0
- ☐ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider

Request hash: Determined by CSP

☐ Use alternate signature format

OK    **Cancel**    Apply    Help

## 6.2.4 Assign permissions to the certificate template

- Click the **Security** tab. Select the Domain Admins and Enterprise Admins groups and uncheck **Enroll** permissions for both these.

Properties of New Template

Subject Name    Server    Issuance Requirements

Compatibility    General    Request Handling    Cryptography    **Security**

Superseded Templates    Extensions    Security

Group or user names:

- Authenticated Users
- tpoadmin (tpoadmin@vprodemo.com)
- Domain Admins (VPRODEMO\Domain Admins)
- Enterprise Admins (VPRODEMO\Enterprise Admins)
- SCS (VPRODEMO\SCS\$)

Add...    Remove

Permissions for SCS

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

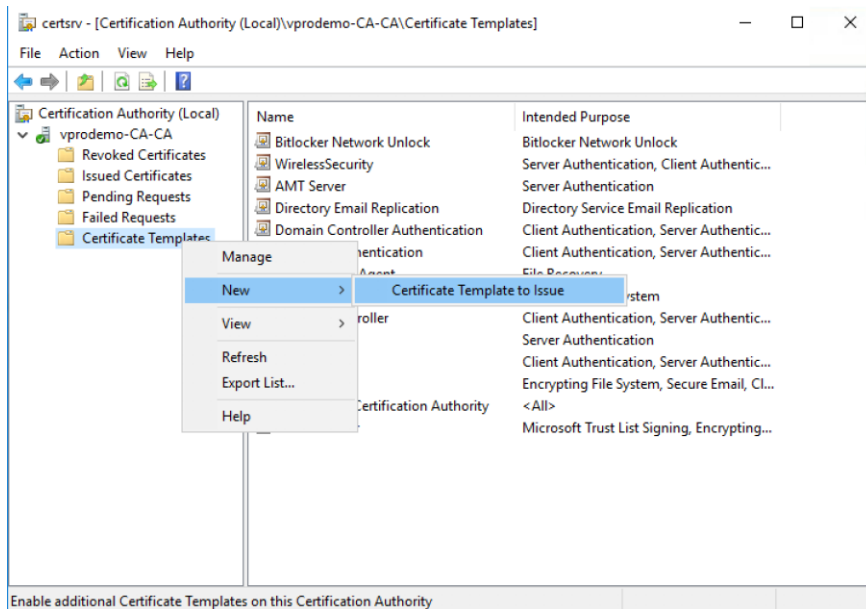
Advanced

OK    **Cancel**    Apply    Help

- Click Add to add the SCS server computer account and check Allow Read and Enroll permissions for this group. Click on the OK button.

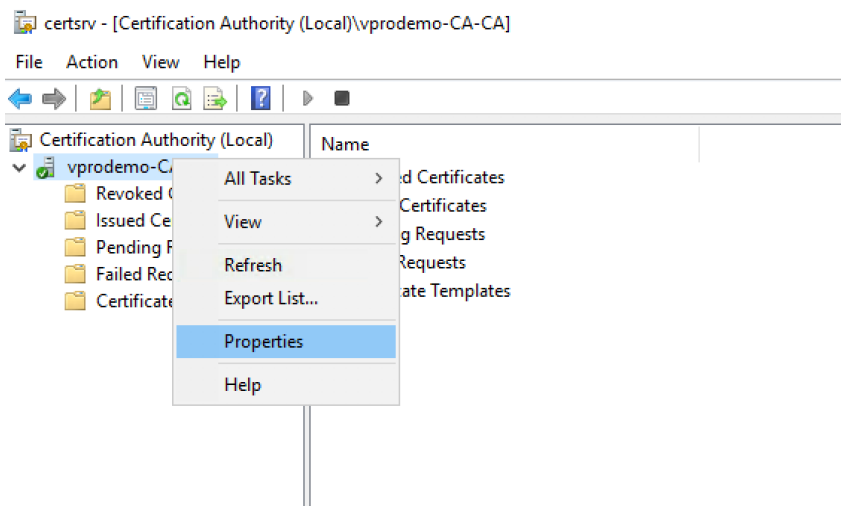
## 6.2.5 Issue certificate template

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.



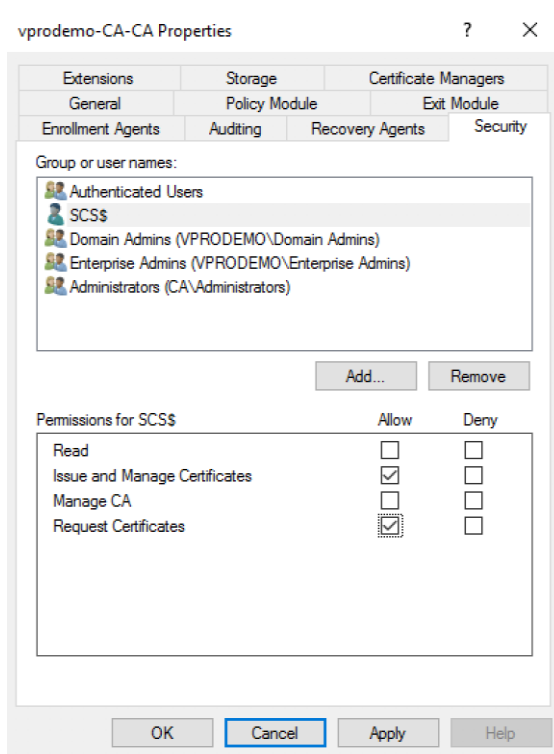
Do not close the Certificate Authority Console.

3. At the CA Console, right-click the CA, in this example **vProLab CA**, and click Properties.



4. Click on the **Security** tab in the CA Properties Window.

- Click **Add** to add the **SCS server computer account** and Allow **Issue** and **Manage Certificates** and **Request Certificates** permissions for this group. Click the **OK** button.

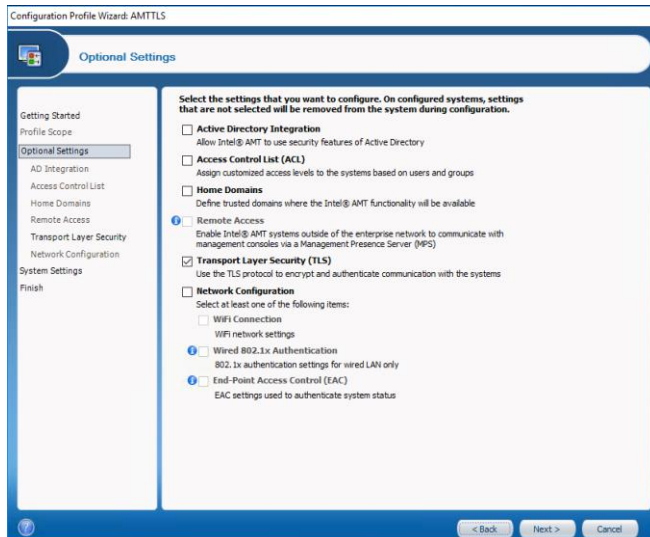


- Close the Certificate Authority Console.
- Restart the CA to publish the new template in Active Directory.

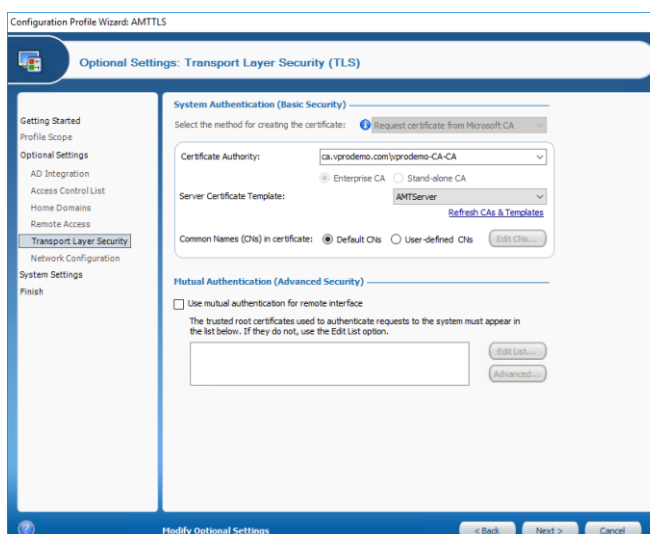
## 6.3 Verify and validate the Transport Layer Security (TLS) configuration

### 6.3.1 Create an Intel® 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



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., AMTServer, as shown below.



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

### 6.3.2 Apply the Intel® AMT profile

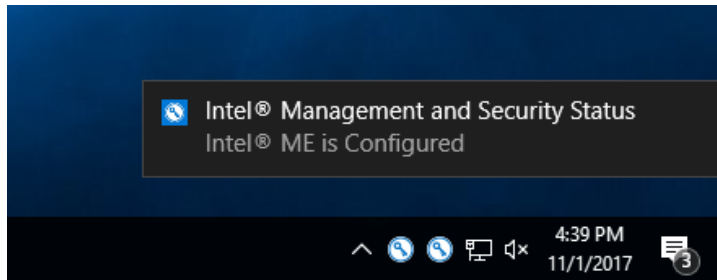
1. Open a command prompt on the Intel® AMT system, using *Run as Administrator*, change to the Configurator directory and execute the following command:

**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**

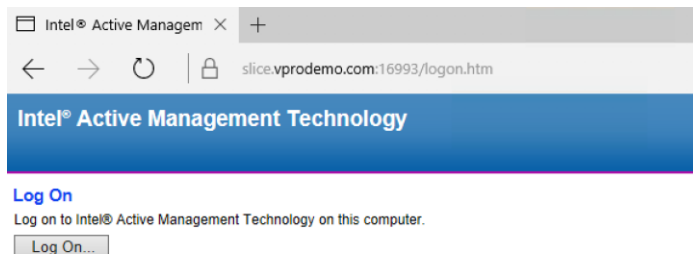
2. When the Intel Management and Security (IMSS) toast notification appears, configuration is complete.



### 6.3.3 Verify Intel® AMT connectivity

1. From the Intel® SCS console system, open a web browser and enter the URL for the Intel® AMT system: **https://FQDN:16993**
2. If the Intel Active Management Technology webpage appears, 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.





## 7 Wireless

### 7.1 Introduction

New innovative form factors and designs for the Intel vPro Platform 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, in combination with Intel® AMT Release 10 and newer, 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 see the *Intel® SCS User Guide* for additional detail.

### 7.2 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.

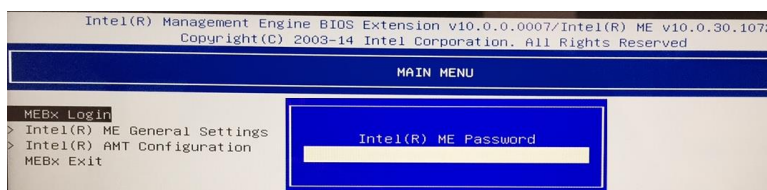
**Note:** Configuration of 802.1x Wi-Fi setups is beyond the scope of this deployment guide. Please reference the Intel® SCS User Guide for additional detail.

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.

#### 7.2.1 PKI DNS Suffix

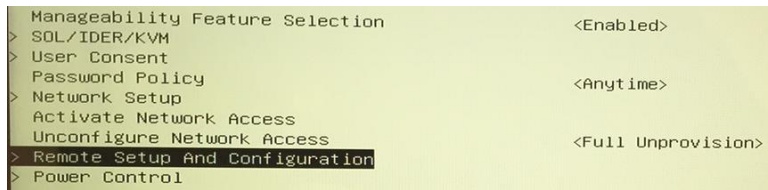
To remotely configure LAN-less Intel® AMT Release 10 and newer systems, the correct PKI DNS Suffix for your organization must be defined within the Intel® MEBX. This section addresses how to manually add this.

1. Enter the Intel® MEBX using the appropriate method dependent upon the OEM, e.g., BIOS menu, <CTRL-P> during system boot, etc.



2. If this is the first time the Intel® MEBX has been accessed, enter the default Intel® ME password (admin). You will then be prompted to set a new Intel® MEBX password.

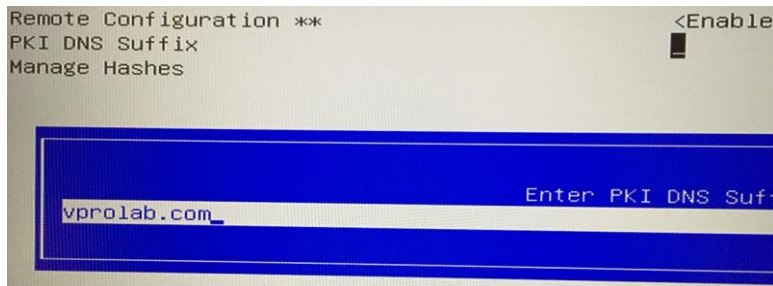
3. Select Intel® AMT Configuration and Remote Setup and Configuration



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 Intel® MEBX menu.

**Note:** When un-configuring Intel® AMT systems, DO NOT perform a full un-provision on a LAN-less system as the PKI DNS Suffix value will be deleted.

## 7.3 Discover

See Section 9.2 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:

Value	Description
WiredLANExists	For LAN-less systems, this value will be "False." The value can also be "True" assuming the next values are configured.
AMTVersion	The version of Intel® AMT.
AMTPKIDNSSuffix	The value defined for the PKI DNS Suffix as defined in the Intel® MEBX

```
<?xml version="1.0" encoding="UTF-8"?>
<SystemDiscovery>
  + <GeneralInfo>
    - <ManageabilityInfo>
      <AMTSKU>Intel(R) Full AMT Manageability</AMTSKU>
      <AMTVersion>10.0.30</AMTVersion>
      <FWVersion>10.0.30.1072</FWVersion>
      <AMTSKUNumber>2</AMTSKUNumber>
    - <Capabilities>
      <IsAMTSupported>True</IsAMTSupported>
      <IsCILASupported>True</IsCILASupported>
      <IsAMTKVMSupported>True</IsAMTKVMSupported>
      <IsTLSSupported>True</IsTLSSupported>
      <IsAntiTheftSupported>False</IsAntiTheftSupported>
      <IsWirelessLANSupported>True</IsWirelessLANSupported>
      <WiredLANExists>False</WiredLANExists>
      <IsCCMSupported>True</IsCCMSupported>
      <IsHBPSupported>True</IsHBPSupported>
      <IsKVMEnabledInBIOS>True</IsKVMEnabledInBIOS>
      <IsKVMSupportedInBIOS>True</IsKVMSupportedInBIOS>
      <IsSOLSupportedInBIOS>True</IsSOLSupportedInBIOS>
      <IsIDERSupportedInBIOS>True</IsIDERSupportedInBIOS>
      <IsAMTEnabledInBIOS>True</IsAMTEnabledInBIOS>
      <IsSOLEnabledInBIOS>True</IsSOLEnabledInBIOS>
      <IsIDEREnabledInBIOS>True</IsIDEREnabledInBIOS>
      <CRLStoreSize>1424</CRLStoreSize>
      <RootCertificatesMaxSize>2500</RootCertificatesMaxSize>
      <RootCertificatesMaxInstances>4</RootCertificatesMaxInstances>
      <FQDNSuffixMaxEntries>4</FQDNSuffixMaxEntries>
      <FQDNSuffixMaxLength>63</FQDNSuffixMaxLength>
      <CertificateChainMaxSize>4100</CertificateChainMaxSize>
    + <SupportedCertificatesKeyLengths>
  </Capabilities>
  - <ManagementSettings>
    <AMTPKIDNSSuffix>vprolab.com</AMTPKIDNSSuffix>
    <AMTConfigurationMode>Enterprise Mode</AMTConfigurationMode>
  </ManagementSettings>
</SystemDiscovery>
```

## 7.4 Remotely configuring LAN-less systems

### 7.4.1 Create an Intel® AMTprofile

1. In the Intel® SCS Console, create a basic profile specifically for LAN-less systems which will be used 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.**"

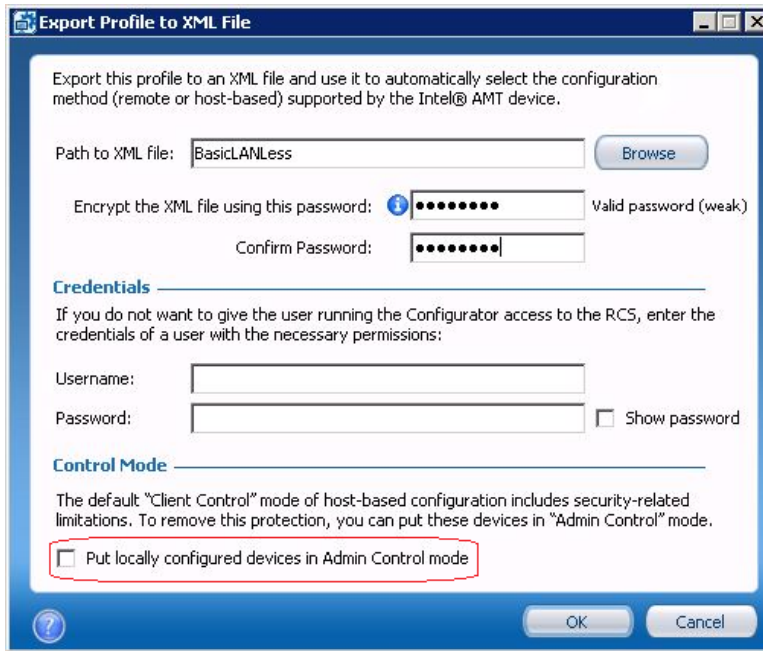
**Note:** Intel® AMT Release 6.0 onwards includes a Wireless Profile Synchronization feature which synchronizes wireless profiles within the operating system with Intel® AMT. To use this feature Intel® PROSet/Wireless Software must be installed on the operating system. For additional information, refer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

- 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 Intel® MEBX.

## 7.4.2 Apply Intel® AMT profile (Host-based configuration)

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

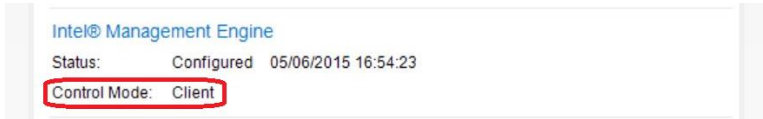
**Note:** Ensure that you do NOT select the check box named Put locally configured devices in Admin Control mode.



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

```
C:\Configurator>ACUConfig /verbose /output console configamt BasicLANLessProfile.xml /DecryptionPassword P@ssw0rd
```

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)



### 7.4.3 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 Intel® MEBX password:

```
C:\Configurator>ACUConfig /verbose /output console movetoacm 192.168.11.35 /AdminPassword 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.

## 8 Configuration

### 8.1 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:

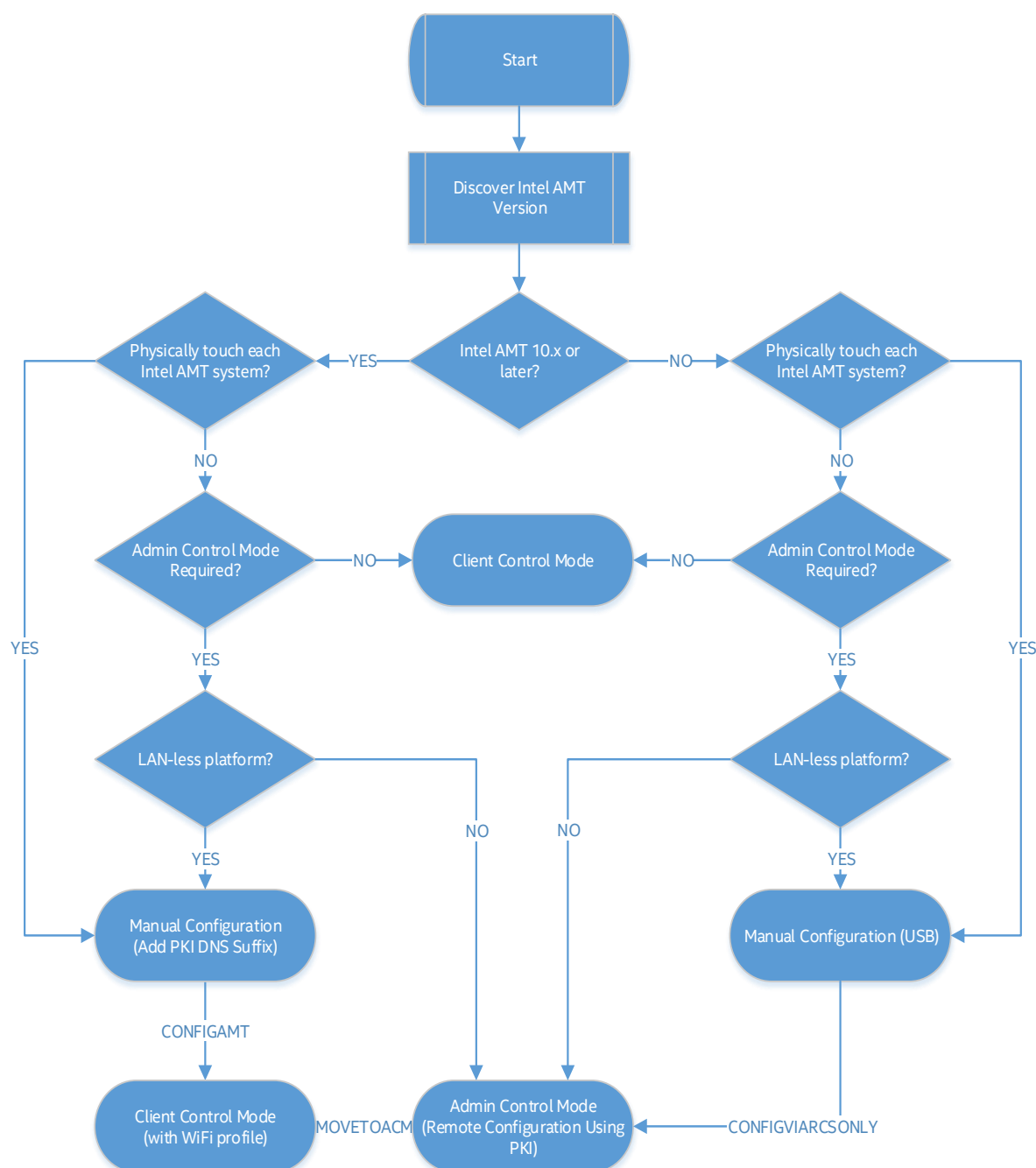
- Deliver an encrypted profile to the target AMT firmware.
- Enable Intel® AMT features and specify behavior.
- Ensure that only authenticated and authorized users can access.

### 8.2 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 in Figure 8-1 provides a simple flow to aid in the selection of a configuration method, all of which result in a configured Intel® AMT system.

**Figure 8-1 Intel® AMT configuration decision tree**



## 8.3 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 GoDaddy, Comodo, and Entrust. 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.

## 8.4 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 Platform, before a remote Intel® AMT session can be established.

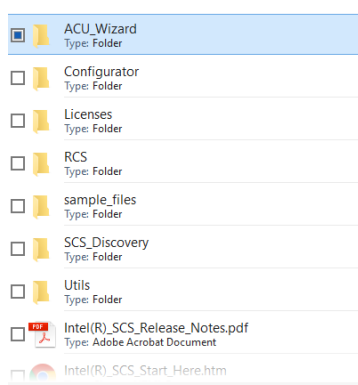
Additional information is available in the *Intel® SCS User Guide*, in the “Configuration Methods and Intel® AMT Versions” and “Control Modes” sections.

## 8.5 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 Intel® 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.
1. Download the entire Intel® SCS package from <http://intel.com/go/scs>.
  2. Extract the **ACU\_Wizard** directory, as selected in the example below and copy to the Intel® AMT client.

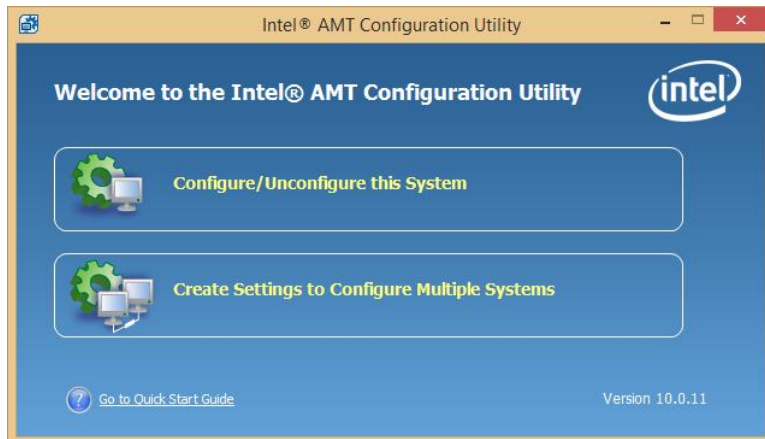
SCS\_download\_package\_12.0.0....



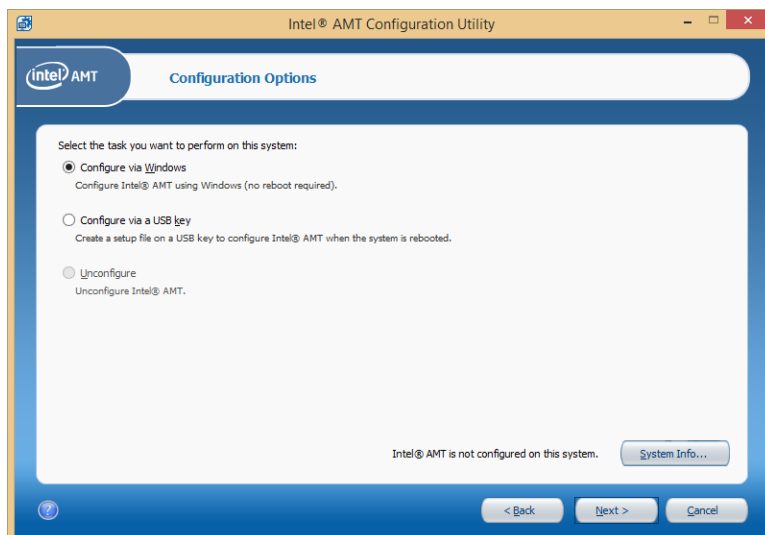
3. On the Intel® AMT system, navigate to the ACU\_Wizard directory and select the executable **ACUWizard.exe**.

**Note:** For systems running Microsoft Windows 7\* 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**.

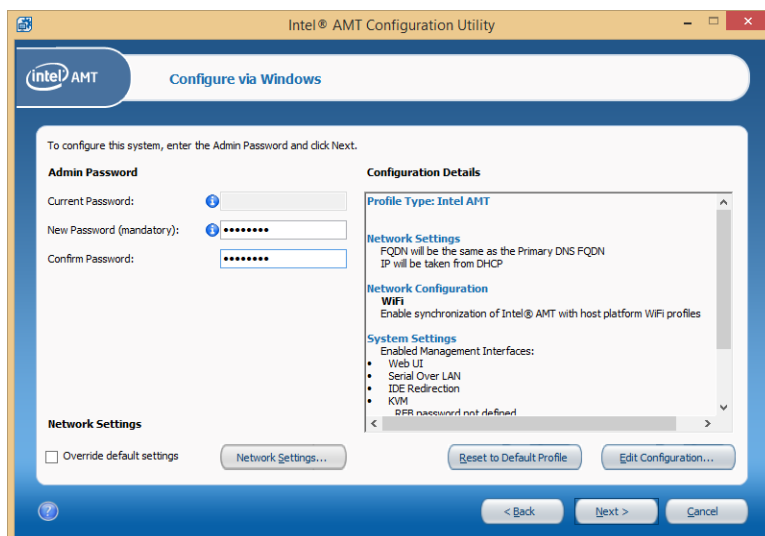
4. When the GUI is displayed, select **Configure/Unconfigure this system**.



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.

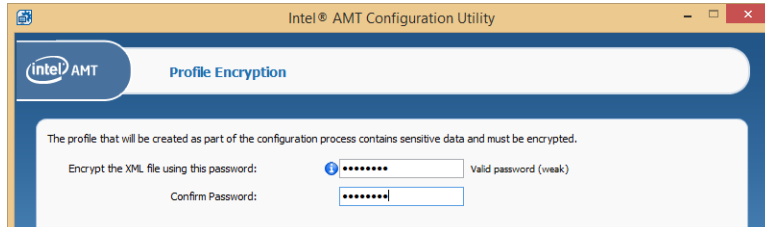


6. For new Intel® AMT systems the default password is **Admin**. Enter a new password and confirm. The existing configuration details should suffice.



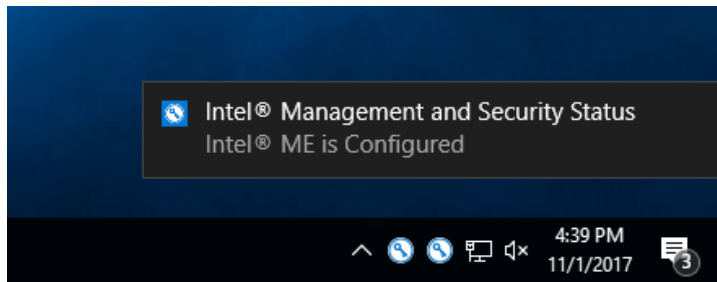
**Note:** The password must be at least 8 and at most 32 characters long, must have at least 1 digit and 1 non-alphanumeric characters and both lowercase and uppercase Latin letters. The underscore (\_) character is counted as alphanumeric.

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

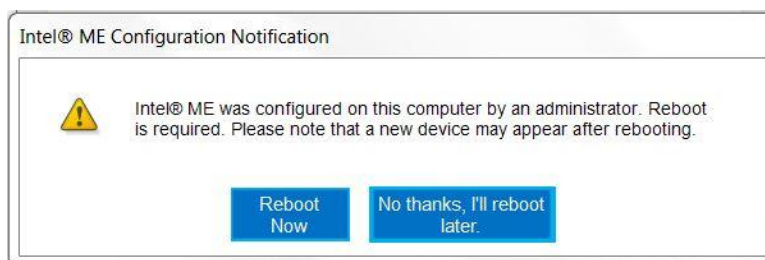


**Note:** **NOTE:** You can use the **SCSEncryption.exe** utility located in the Utils folder of the Intel® SCS download package to encrypt and decrypt files using the same format used by Intel® SCS. For more information, refer to the CLI help of the **SCSEncryption.exe** utility.

8. Click the **Configure** button and Intel® AMT will begin configuration.
9. When the Intel Management and Security (IMSS) toast notification appears, the Intel Management Engine (Intel® ME) configuration is complete.



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



For troubleshooting purposes, you can locate this operation 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.

## 8.6 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.

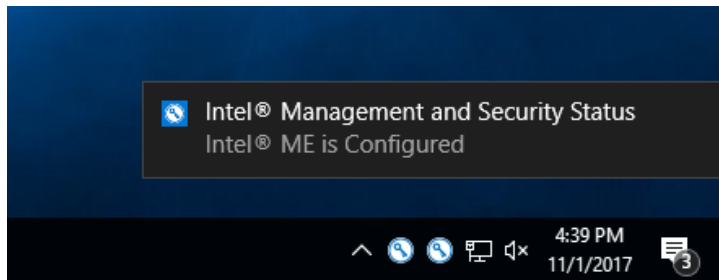
**Note:** For systems running Microsoft Windows 7\* or newer operating systems, this executable must be opened with elevated privileges due to interaction with a kernel level driver. This is

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) toast notification appears, the Intel Management Engine (Intel® ME) configuration is complete.



For troubleshooting purposes, you can locate the log corresponding with this operation in the **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.

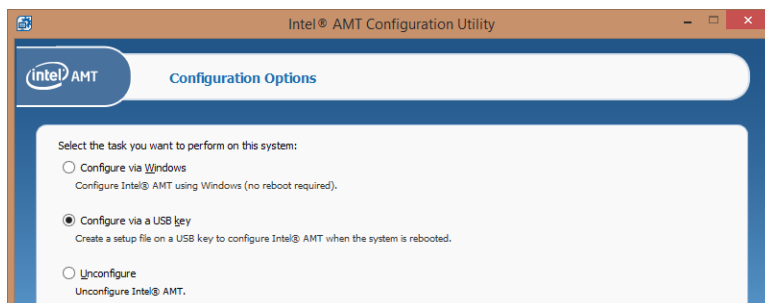
## 8.7 Manual configuration

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 Intel® 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.

**Intel® MEBX Password**

Current Password:  ☒ Show password

New Password:

Confirm Password:

☒ Display advanced settings

**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.

**Power Settings**

Specify the system power states in which the Intel® Management Engine is operational:

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.

**Network Settings**

Hostname:

Domain name:

☒ DHCP Enabled

IP:

Subnet mask:

Gateway:

Primary DNS:

Secondary DNS:

- **Redirection Settings:** These settings are only shown for systems with Intel® AMT 6.0 and newer.

**Redirection Settings**

☒ Enable KVM Redirection

☒ Allow IT to change user consent setting

User consent setting:

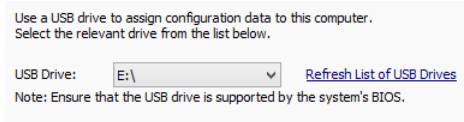
☐ User consent not required

☒ User consent required for KVM sessions

☐ User consent required for all redirection operations

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.

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



- Click the **Next** button and a message is displayed warning that the USB key will be formatted.
- 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.
- Click the **Finish** button and the Configuration Utility closes.
- Ensure that only the USB key that you created is connected to the target Intel® AMT system and reboot.
- During the reboot, a message is shown on the screen:

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

- 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...
```

- 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.

## 8.8 Manual configuration (multiple systems)

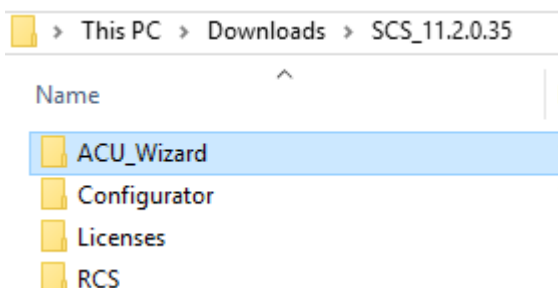
Alternatively you can prepare a USB key with identical configuration settings to use with multiple Intel® AMT systems. When the systems are rebooted with the USB key, Intel® AMT is configured.

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.

## 8.9 Unconfigure method

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

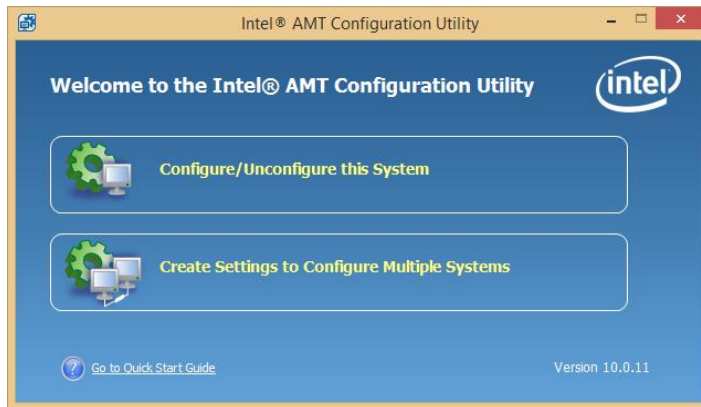
- Extract the **ACU\_Wizard** directory, as selected in the example below and copy to the Intel® AMT system.



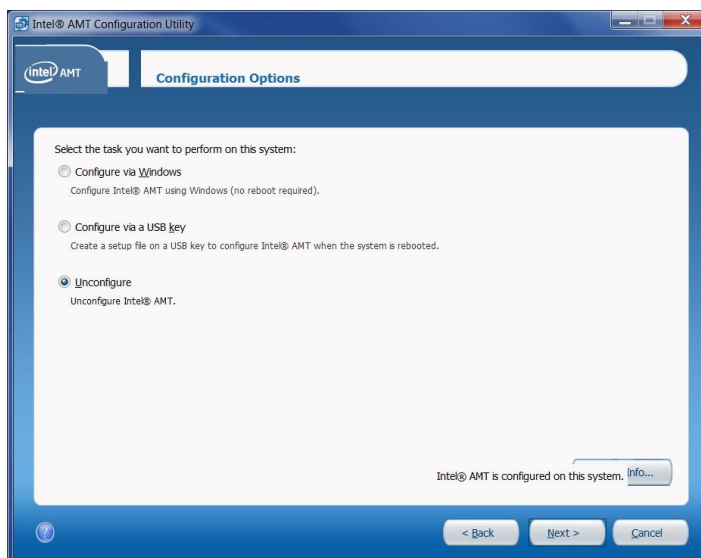
2. On the Intel® AMT system, navigate to the ACU\_Wizard directory and select the executable **ACUWizard.exe**.

**Note:** For systems running Microsoft Windows 7\* 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**.

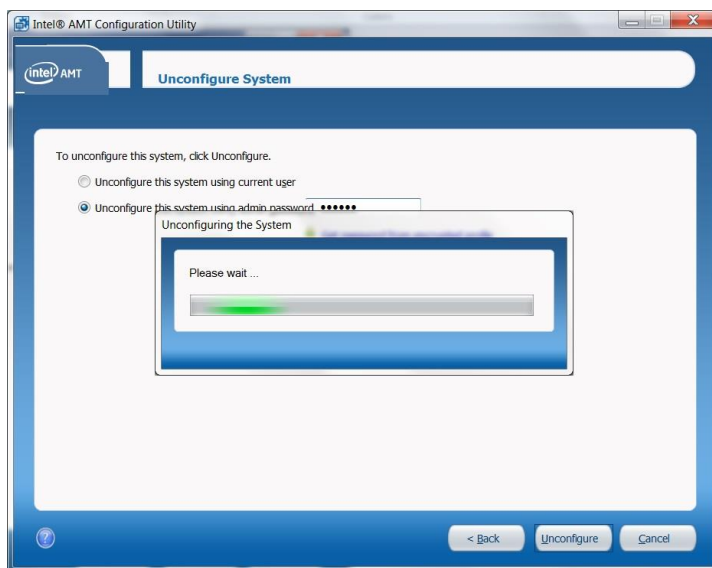
3. When the GUI is displayed, select **Configure/Unconfigure this System**.



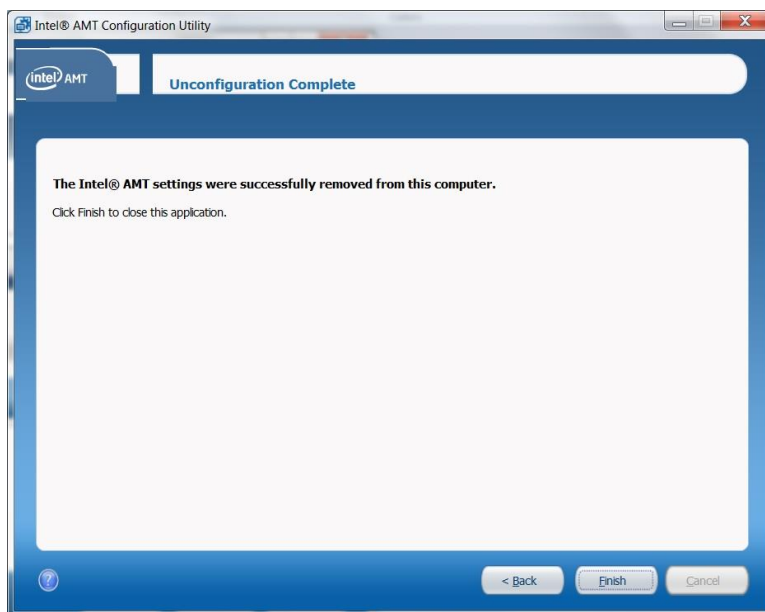
4. Select **Unconfigure** and click the **Next** button.



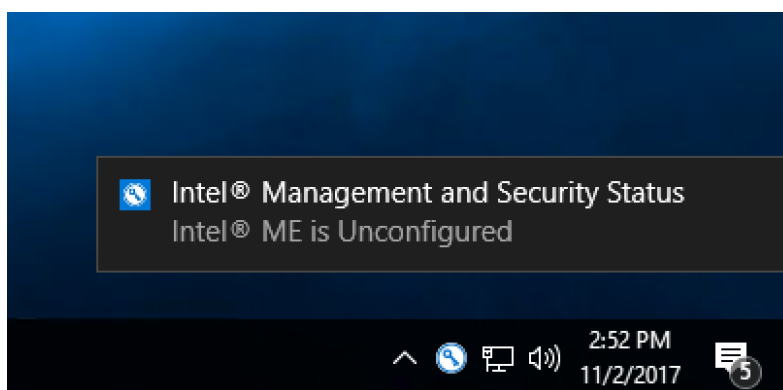
5. Select **Unconfigure this system using admin password**, enter the admin password (P@ssw0rd), and click the **Next** button.



6. Once complete, Intel® AMT will be unconfigured and un-provisioned. Click the **Finish** button.



The Intel Management and Security Status toast notifies you that the Intel® ME is Unconfigured.





## 9 Discovery

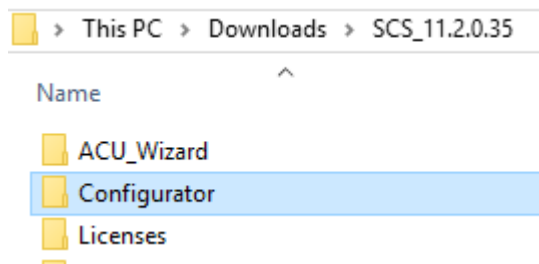
### 9.1 Introduction

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.

### 9.2 Using the configurator

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

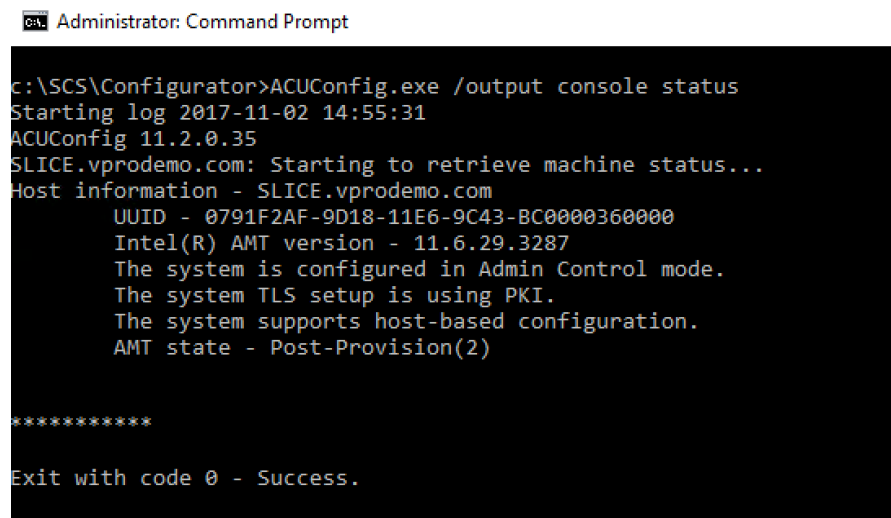


3. On the Intel® AMT system, open a command prompt to the **Configurator** directory.

**Note:** For systems running Microsoft Windows 7\* 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



```
Administrator: Command Prompt

c:\SCS\Configurator>ACUConfig.exe /output console status
Starting log 2017-11-02 14:55:31
ACUConfig 11.2.0.35
SLICE.vprodemo.com: Starting to retrieve machine status...
Host information - SLICE.vprodemo.com
  UUID - 0791F2AF-9D18-11E6-9C43-BC0000360000
  Intel(R) AMT version - 11.6.29.3287
  The system is configured in Admin Control mode.
  The system TLS setup is using PKI.
  The system supports host-based configuration.
  AMT state - Post-Provision(2)

*****

Exit with code 0 - Success.
```

In the above example, the output of the ACUconfig.exe Status command shows that the Intel® 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:

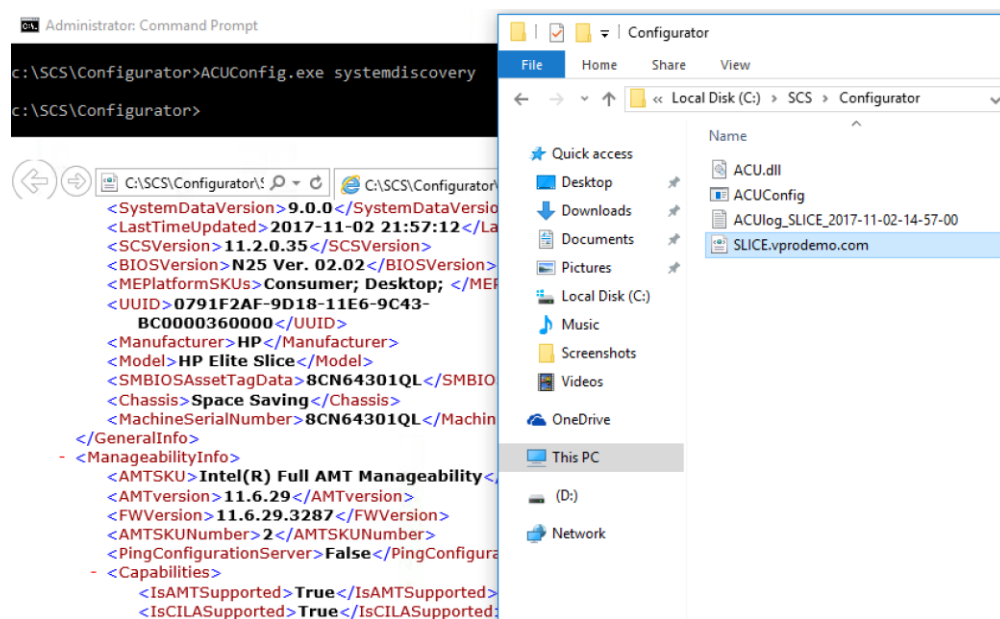
**HKLM\SOFTWARE\Intel\Setup and Configuration Software\SystemDiscovery**

In addition, on 64-bit operating systems:

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

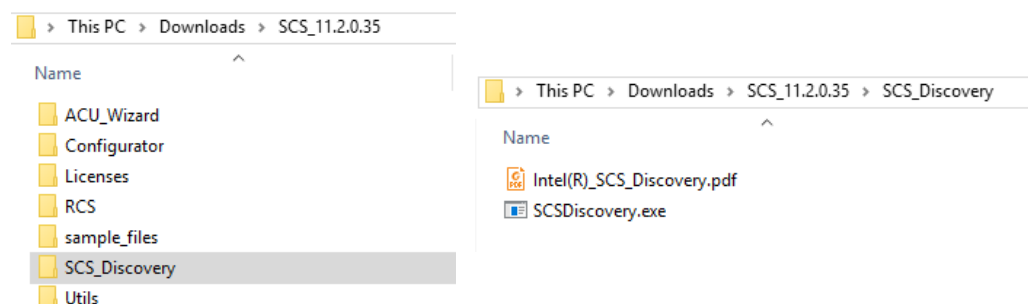
The resulting data provides an in-depth view of the Intel® AMT platform in a format which can be centrally collected via custom inventory solutions. Figure 3 shows the resulting XML file located in the Configurator directory and a preview of the file contents. The combined information is helpful with 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.”



## 9.3 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.

## 9.4 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.”

## 9.5 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 Intel® SCS Platform Discovery download at <https://www.intel.com/go/SCS>.



```
<PlatformDiscovery version="10.0.11.35">
  <Framework available="false"/>
  <Solution uuid="a543b148-407c-419d-ab91-6a26af664828" name="Intel(R) Smart Connect Technology" exist="false" state="not supported"/>
  <Solution uuid="a5e80b51-5429-4904-b412-589470884e97" name="Intel(R) AMT" exist="true" managed="true" state="configured">
    <Hardware version="Intel(R) ME- 10.0.30.1072"/>
    <Software name="Intel(R) Management Engine Interface " required="true" available="true" version="10.0.30.1054"/>
    <FrameworkPlugin available="false"/>
  </Solution>
  <Solution uuid="0b93a9cb-64b1-43ed-bc33-e5b0b8692694" name="Intel(R) SSD Pro Series" exist="false" state="not supported"/>
  <Solution uuid="8f14b6c3-9981-4347-8f05-08582591f486" name="Intel(R) Anti-Theft Technology" exist="true" managed="false" state="not-enrolled">
    <Hardware version="Unknown version"/>
    <FrameworkPlugin available="false"/>
  </Solution>
  <Solution uuid="8d101420-2d30-4ff4-b18a-1da73e67d0ef" name="Location Based Service" exist="true" managed="false" state="supported">
    <Hardware version="Intel(R) Dual Band Wireless-AC 7265"/>
    <Software name="Intel(R) Dual Band Wireless-AC 7265" required="true" available="true" version="17.12.0.6"/>
    <Software name="Intel(R) PROSet/Wireless Zero Configuration Service" required="true" available="true" version="17.12.0.0"/>
    <Software name="Microsoft Windows 7 Professional 64-bit" required="true" available="true" version="6.1.7601"/>
    <FrameworkPlugin available="false"/>
  </Solution>
  <Solution uuid="a8c6bb4d-eda0-4859-bc7a-197cf252cf88" name="Intel(R) Enterprise Digital Fence" exist="false" state="not supported"/>
  <Solution uuid="7144b5b8-6883-44a9-80a2-c112ae6d6d7f" name="Intel(R) IPT with OTP" exist="true" managed="false" state="supported">
    <Hardware version="Intel(R) ME- 10.0.30.1072"/>
    <Hardware version="Intel(R) Core(TM) i5-4310U CPU @ 2.00GHz"/>
    <Software name="Intel(R) Management Engine Interface " required="true" available="true" version="10.0.30.1054"/>
    <FrameworkPlugin available="false"/>
  </Solution>
  <Solution uuid="34e60d6a-457a-483b-82ee-cb4f5ba6f542" name="Intel(R) IPT with PKI" exist="true" managed="false" state="supported">
    <Hardware version="Intel(R) ME- 10.0.30.1072"/>
    <Hardware version="Intel(R) Core(TM) i5-4310U CPU @ 2.00GHz"/>
    <Software name="Intel(R) Management Engine Interface " required="true" available="true" version="10.0.30.1054"/>
    <FrameworkPlugin available="false"/>
  </Solution>
  <Solution uuid="89f11f6d-f4a4-4379-a4cd-8bde2d0d6b8a" name="Intel(R) IPT with MFA" exist="true" managed="false" state="supported">
```

## 9.6 Using the Solutions Framework

This is not covered in this guide. For more information, please refer to the documentation in the Solutions\_Framework download at <https://www.intel.com/go/SCS>.