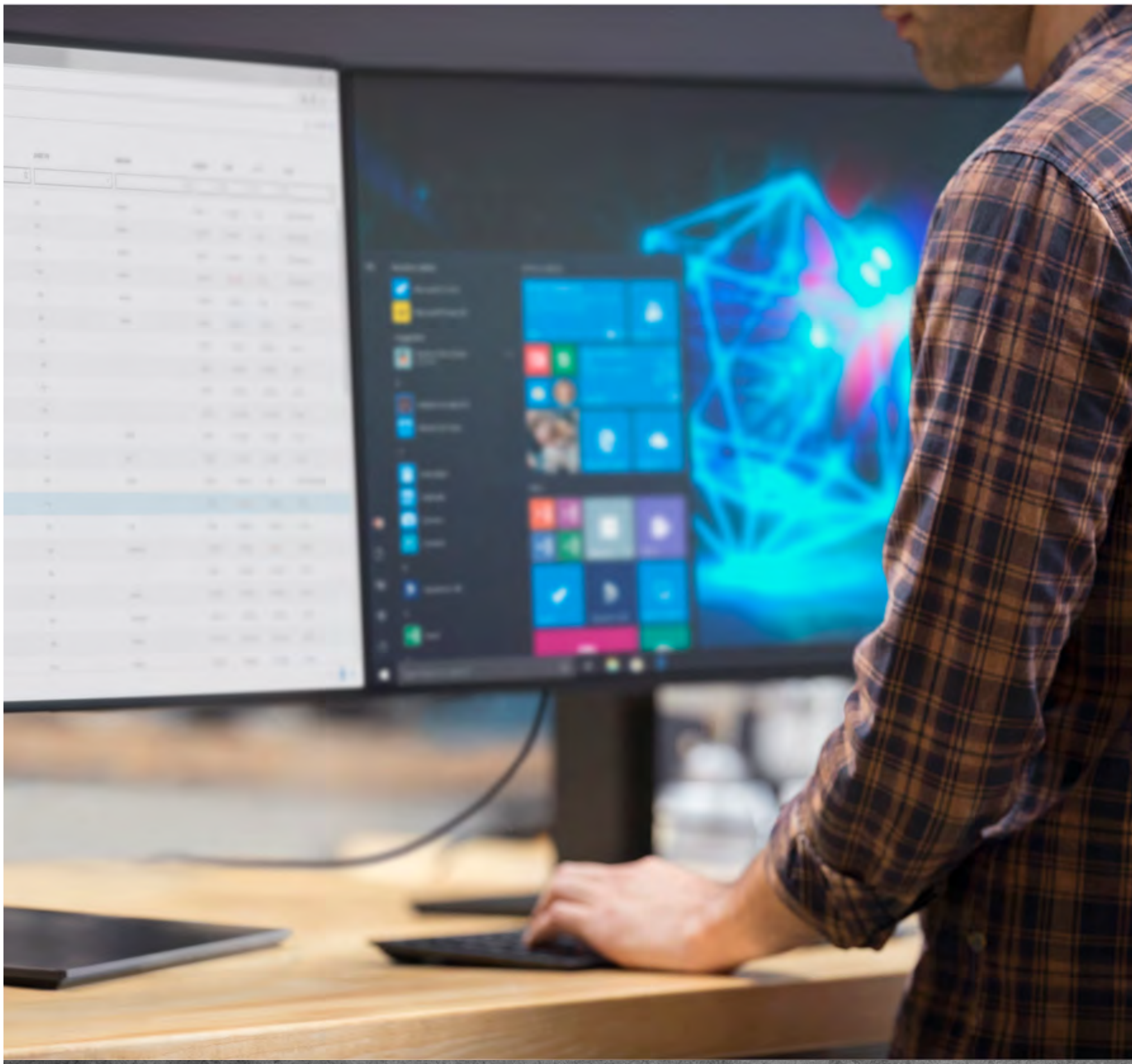
TECHNICAL
WHITE PAPER

CONTENTS & NAVIGATION



INTEL® AMT ENTERPRISE PROVISIONING

PURPOSE OF THIS DOCUMENT

When configuring Intel® Advanced Management Technology (Intel® AMT), there are different options for enabling network access so that client devices can be remotely managed. With the ZCentral solution, the Intel® AMT capabilities can be used to better manage a fleet of Z Workstations. This document breaks down the steps involved with setting up network access, or provisioning, such that Intel® AMT features can be used with ZCentral Connect. The enterprise-level provisioning methods described in this document are tested by HP as part of the ZCentral solution validation, however there may be other methods for provisioning AMT, such as manual provisioning methods that may make deploying AMT more difficult. For example, the simplest form of manual provisioning would require that each AMT device be physically accessed and booted to a USB drive with a provisioning file, which can be burdensome if entire fleets of systems are to be deployed.

BENEFITS OF ENTERPRISE PROVISIONING

Enterprise provisioning of AMT is required to enable some of the manageability and health monitoring features of ZCentral Connect. HP ZCentral software requires Transport Layer Security (TLS) encryption for any communication with AMT devices on remote machines. Kerberos is also the default, and recommended, option for authentication. Kerberos is not able to be configured without enterprise provisioning.

When enterprise provisioning is performed, the AMT device is automatically placed in Admin Control Mode (ACM) which is required for remotely managing ZCentral Workstations.

Manually provisioning AMT, the alternative to enterprise provisioning, requires Intel® AMT to first be enabled in the F10 BIOS Menus. Then to provision AMT requires entering the MEBx menu, by pressing F6, during POST or booting the machine to a USB drive with a provisioning file. To enable TLS requires extra steps using third party tools to reach each AMT device individually. Enterprise provisioning simplifies the process and save time when there are more than a handful of AMT devices to provision.

INTEL® AMT NETWORK STRATEGY

The use of Intel® AMT in conjunction with ZCentral software is done such that the AMT-enabled devices only have an AMT connection with the ZCentral Connect manager. All AMT communication can therefore stay within the ZCentral network. All AMT operations (e.g. Powering on an AMT device), are orchestrated through the ZCentral Connect manager. For example, an end user wanting to power cycle a workstation initiates the request through the ZCentral Connect client portal, and then the ZCentral Connect manager sends the AMT remote power command. Since the ZCentral Connect manager controls the messaging between AMT devices and the end-user, only the ZCentral Connect manager requires the credentials to access AMT on the devices being managed. The ZCentral Connect manager and AMT devices communicate by default over ports 16992 and 16993, and the ZCentral team recommends verifying that these ports are open between the ZCentral Connect manager and the ZCentral Workstations.

INTEL® TOOLS FOR ENTERPRISE PROVISIONING

The Intel® Setup and Configuration Software (SCS) and the Remote Configuration Server (RCS) applications are required for enterprise provisioning. The RCS is a service that listens for provisioning requests and directly applies a configuration profile to the target AMT device. The SCS provides a console to manage the RCS, including creating configuration profiles and monitoring the provisioning process for remote machines. Maintenance tasks can be scheduled with SCS, which are acted upon by the RCS. Maintenance tasks include reissuing TLS server certificates to provisioned AMT devices or fixing FQND mismatches.

The SCS package contains the RCS and they share a single installer. The package can be obtained from the Intel® website.

To monitor provisioned AMT devices or perform maintenance tasks, RCS needs to be connected to an SQL server. Note that an SQL server is not required for the provisioning steps.

PRE-REQUISITES AND OPTIONAL SOFTWARE COMPONENTS

Environment Pre-requisites

- Active Directory domain with Domain Controller running Windows Server 2012 or newer is required to enable enterprise provisioning
- DNS Server is needed for FQDN retrieval
- DHCP Server to assign AMT devices' IP address, and for devices to retrieve the domain name
- Enterprise Certificate Authority to enable Transport Layer Security
- Windows Server 2016 or Windows 10 host for RCS

Optional Environment Components

- SQL Server is used by Intel® RCS to maintain information on provisioned machines and allow for maintenance jobs to be scheduled
- SCCM to automate the provisioning process for AMT devices
- SCS Add-on for SCCM to simplify SCCM task sequences and provide classes for AMT provisioning

Other Tools that May Be Used

Since Intel® AMT is disabled by default on modern Z Workstations, it may be desirable to use a tool that can remotely enable AMT in BIOS. This operation can be done manually by going into the F10 BIOS Menus during POST, and in the Advanced Tab, under Remote Management Options, Intel® AMT can be enabled by checking the box next to, “Intel® Active Management Technology (AMT)”.

One tool that HP provides for locally, or remotely, configuring BIOS settings is the HP BIOS Configuration Utility (BCU). The utility is supported for both Windows and Linux operating systems, and both the utility and documentation on how to use the utility can be found here: **https://ftp.hp.com/pub/caps-softpaq/cmit/HP_BCU.html**

Using the BCU tool, the Intel® Active Management Technology (AMT) option can be changed from Disabled (Default setting) to Enabled.

DIFFERENT TYPES OF ENTERPRISE PROVISIONING

Enterprise Provisioning can be accomplished in different ways. Private Shared Key (PSK) and Public Key Infrastructure (PKI) are the base methods. PSK was removed in AMT 11.0 and is not recommended by Intel®. The PKI method can be performed in 2 main ways, using the AMT Config Utility (ACU) or using Hello Packets. Both methods require Intel® SCS and RCS. Both also require a provisioning certificate. The onetime setup process is generally the same.

The differences between the two methods is most noticeable when it comes time to provision each AMT device. With the ACU method provisioning is requested by an application running in the remote machine’s OS (Windows only).

If a Windows OS is not installed, the ACU method can still be accomplished by booting to a WinPE image from a removable storage device (USB) or Preboot Execution Enviornment (PXE) server. The WinPE environment can simply be used to host the ACU provisioning method.

The Hello Packet method allows for “Bare Metal” and does not require an OS to be installed. In both cases the RCS receives a request and communicates with the AMT device directly to complete provisioning.

The following is the step by step instructions required to use enterprise provisioning for Intel® AMT.

ACU Provisioning:

One Time Setup:

1. Obtain Provisioning Certificate.
2. Add Option 15 to DHCP.
3. Create RCS Service Account.
4. Create Security Group to give Kerberos access to devices on the network.
5. Create Organization Unit (OU) in AD for provisioned machines.
6. Create Certificate Template for AMT Server Certificates.
7. Create Certificate Template for AMT Client Certificates.
8. Install Intel® SCS.
9. Create Configuration Profile.
10. Set RCS Advanced Configuration Options.

Each Machine Setup:

1. Enable AMT in BIOS Menus[1].
2. Ensure Provisioning Certificate is trusted by AMT Device[1].
3. Boot to OS.
4. Request Provisioning.

Hello Packet Provisioning:

One Time Setup (Differences from ACU provisioning in bold):

1. Obtain Provisioning Certificate.
2. Add Option 15 to DHCP.
3. **Add Alias to the RCS Server in DNS.**
4. Create RCS Service Account.
5. Create Security Group to give Kerberos access to devices on the network.
6. Create Organization Unit (OU) in AD for provisioned machines.
7. Create Certificate Template for AMT Server Certificates.
8. Create Certificate Template for AMT Client Certificates.
9. Install Intel® SCS.
10. Create Configuration Profile.
11. **Create script to gather information unavailable from Hello Packets.**
12. Set RCS Advanced Configuration Options.

Each Machine Setup:

1. Enable AMT in BIOS Menus[1].
2. Ensure Provisioning Certificate is trusted by AMT Device[1].
3. **Enable Hello Packets[1].**

Note 1: The enablement of AMT, setting up the MEBx password, and loading of provisioning certificates are services that the HP Custom Services team are set up to do. Please contact your HP sales representative for more details. This service would allow for systems to be remotely provisioning upon installation to your provisioning network.

SETUP STEP DETAILS

Obtain Provisioning Certificate

About Provisioning Certificate

To ensure security, a provisioning certificate is required for the AMT devices to trust the remote configuration server. Trust is validated similarly to TLS. Before provisioning is allowed the RCS sends the provisioning certificate along with the certificate chain to the AMT device. The AMT device validates the certificate in the following ways:

- Ensures the certificate is an SSL Server Certificate
- Ensures that the certificate contains the correct Object Identifier (OID) or Organizational Unit (OU) attribute that marks it for provisioning AMT devices
- The certificate's chain of trust ends with a Root Certificate Authority that is trusted by the AMT device
- The FQDN suffix on the certificate matches the Domain Name from DHCP option 15
  - This can also be set directly within MEBx if DHCP option 15 is unavailable

The chain of trust is validated by certificate hashes that are held by the AMT device. There can be up to active 23 total hashes per AMT device (including any preinstalled hashes that are active). There are 20 preinstalled in AMT devices from the most common certificate providers (e.g. VeriSign, GoDaddy, Comodo, Starfield, Entrust, Affirm Trust, Verizon, Cybertrust Global, Baltimore CyberTrust, GTE CyberTrust). Custom certificate hashes can be added and active as well. These custom hashes must be added through the MEBx menu manually or through a USB configuration file.

How to Obtain

The common certificate providers mentioned above will sell AMT provisioning certificates, issued by their root certificates already trusted by AMT devices. The process to request the certificates is different per provider and are custom to each RCS instance. The FQDN of the host on which the RCS runs will have to be provided during the purchase.

A custom certificate can be created using an internal CA as well. These are the generic steps:

1. On a domain controller, go to the Certificate Authority tools and then select, Manage the Certificate Templates.
2. Find the Web Server template and duplicate it.
3. Change the template name to something that makes sense for your Provisioning Certificate.
4. Under Request Handling make sure the private key can be exported.
5. On the Subject Name tab choose, Build from this Active Directory Information and select Common Name.
6. On the Extensions Tab add a new Application Policy with an OID of 2.16.840.1.113741.1.2.3 (this value must match to be recognized by the AMT device):
   a) Select Application Policies and click Edit
   b) On the Edit Application Policies Extension window click Add
   c) On the Add Application Policy window click New
   d) Enter a Name that makes sense and the OID
   e) Click Ok until you are back to the New Template window
7. Under the Security Tab make sure that the certificate is able to be requested by the administrator account setting up the RCS.
8. Issue the newly created template.

How to Use

The account running the RCS (specified at install time) needs to have access to the public and private keys of the provisioning certificate, along with the public keys of all intermediate certs and the root cert. The easiest way to accomplish this is to place the Provisioning Certificate into the Personal certificate store for the account in Windows. All intermediate and root certs need to be placed in the "Intermediate Certification Authorities" and "Trusted Root Certification Authorities" stores respectively. If this is done the RCS is able to send the required information to authenticate to the AMT device.

If accessing the personal store is unavailable due to the type of account used (e.g. Network Service account) Intel® SCS contains a tool called RCSUtils.exe which can be used to add certificates to the required accounts.

Add Option 15 to DHCP

The AMT device needs to know the name of the domain in which the RCS server is installed to validate the Provisioning Certificate. Because the AMT device is separate from the OS this name has to be accessed in some other way. One possibility is to manually enter the domain name suffix in MEBx. To avoid the manual step, and to enable zero-touch provisioning DHCP can be used. DHCP Specification Option 15 provides the domain name to any device (including the AMT device) getting assigned an IP.

Add Alias to the RCS Server in DNS

When the Hello Packet provisioning method is used, the AMT device needs to know where the RCS is listening on the network. Through the MEBx menu the FQDN or the IP address of the RCS can be entered. Just like with the domain name suffix this requires a manual step for each AMT device. To avoid the manual step, and to enable zero-touch provisioning using a DNS alias can help. If no FQDN is specified in MEBx, hello packets are sent over the network to the "ProvisionServer" address. Adding an alias in DNS to the RCS machine as "ProvisionServer" ensures that the hello packets are sent to the correct IP address.

Create RCS Service Account

The RCS must be run using a service account. This can be a domain account or the built in "Network Service" account in which no creation is necessary. This account must be given permissions to manage the OU in AD and request certificates needed to provision AMT (both explained in other sections). For more information see the RCS User Account Requirements section in the Intel® SCS User Guide.

Create Security Group to give Kerberos access to devices on the network

There are multiple ways to give Kerberos access to an account with configuration profiles. A good practice to follow is to create a normal security group in AD and give that group access. This way, users and other groups can be added or removed without re-provisioning all AMT devices.

Create an Organization Unit (OU) in AD for provisioned machines

For Kerberos to work the Service Principles for the provisioned AMT devices needs to be held in AD. The RCS manages these AD objects but when creating a configuration profile an OU needs to be defined where the account running the RCS has access.

These are example steps:

1. On a domain controller, open ADSI Edit.
2. Create a new OU and give it a name such as "AMT Provisioned Devices".
3. Go to the properties of the new OU.
4. Under the security tab add the account running the RCS.

Create Certificate Template for AMT Server Certificates

To enable TLS communication the RCS needs to be able to get a certificate issued by the domain's Certificate Authority (CA). A special certificate template just for AMT TLS should be used to ensure the correct settings are used. When a device needs to be provisioned the RCS will request and be issued one of these certificates. It will then push it to the AMT device during configuration. Any application will need to validate this certificate with the normal TLS protocols to ensure authentication.

These are the steps to create the Server Certificate Template:

1. On the domain controller go to the Certificate Authority Tools and then Manage the Certificate Templates.
2. Find the default Web Server template and duplicate it.
3. Change the template name to something that makes sense for an AMT Device's server certificate (e.g. AMT Server Certificate).
4. Check the "Publish certificate in Active Directory" box.
5. Under Request Handling make sure the private key can be exported.
6. On the Cryptography tab make sure Microsoft Strong Cryptographic Provider is one of the selected providers.
7. On the Subject Name tab choose to supply the subject in the request.
8. Ensure that the "Server Authentication" application policy (OID: 1.3.6.1.5.5.7.3.1) is being used.
9. Under the Security Tab give full permissions to the account running the RCS.
10. Issue the newly created template.

Create Certificate Template for AMT Client Certificates

During a TLS negotiation the client will request the server certificate from the server (In this case the AMT device). The client validates the certificate and then the encryption key is generated, and secure communication occurs. There are cases where the server wants added authentication and will also request a certificate from the client that it then verifies. This is called "mutual Transport Layer Security" or mTLS. AMT supports mTLS and it can be enabled by enterprise provisioning. When it is enabled any application attempting to connect as a client to the AMT device will need to present a certificate, the Root CA that issued it, and any intermediate certificates in the chain. The AMT device can be configured to trust a Root CA for mutual authentication. Note, this is a different validation than the one done for a provisioning certificate and pre-installed certificate hashes are not used.

A certificate template can be used to request these client certificates in an enterprise CA. Here are the steps to create the template:

1. On the domain controller go to the Certificate Authority tools and then Manage the Certificate Templates.
2. Find the default Web Server template and duplicate it.
3. Change the template name to something that makes sense for an AMT client certificate (e.g. AMT Client Certificate).
4. Check the "Publish certificate in Active Directory" box.
5. Under Request Handling make sure the private key can be exported.
6. On the Cryptography tab make sure Microsoft Strong Cryptographic Provider is one of the selected providers.
7. On the Subject Name tab choose to supply the subject in the request.
8. Ensure that the "Server Authentication" application policy (OID: 1.3.6.1.5.5.7.3.1) is being used.
9. Add a new Application Policy with an OID of 2.16.840.1.113741.1.2.1
   a) Select Application Policies and click Edit
   b) On the Edit Application Policies Extension window click Add
   c) On the Add Application Policy window click New
   d) Enter a Name that makes sense and the OID
   e) Click ok all the way back to the New Template window
10. Under the Security Tab give full permissions to any account needing to authenticate to an AMT device as a client (e.g. Service Account running ZCentral Connect).
11. Issue the newly created template.

Install Intel® SCS

Installing SCS is a relatively simple step in the process. Here is an example of installing with SCS version 12:

1. In the SCS download package go to the RCS directory and run the **Intel® SCS Installer** application.
2. Accept the terms of the license agreement.
3. When Selecting Components make sure Remote Configuration Service and Console are both selected.
   a) Database Mode should be used if possible, to keep track of provisioned machines and allow for maintenance tasks
      i. Database Mode requires an SQL server
   b) NOTE: If using AMT versions older than 11 in the environment make sure to support TLS 1.0 for backwards compatibility
4. Use the desired account to run the RCS.
5. On the Database Settings page enter the FQDN of the SQL Server and enter the required credentials.
   a) The installer will create the SQL Database
6. Confirm the Installation path and hit Install.
7. Wait for the installation to finish and close the installer.

After installation is complete the RCS service will be running, and the SCS console can be launched to manage it.

Create Configuration Profile

A configuration profile is a selection of settings used by the RCS to configure an AMT device. To create a new configuration profile, open the SCS console, navigate to the Profiles screen, and press the green “+” button. A wizard will provide guidance throughout the process of creating the profile.

Settings used for Z Workstations that will be used with ZCentral Connect should setup AD Integration, Access Control List, and Transport Layer Security in the profile. The SCS Console tabs are described in the subsections below. For detailed information on all configuration profile options see the Intel® SCS user guide.

AD Integration Tab

Active Directory Integration is required for Kerberos authentication. In addition, this is needed for 802.1x protocol and End-Point Access Control features if required by the enterprise environment. During provisioning the RCS will create a new AD computer object for the AMT device. This AD object contains attributes required for Kerberos authentication. The only setting needed to enable AD Integration is to specify an OU from AD. This is the Organizational Unit created in a previous step.

Please note, the “Always use the OS Host Name for the new AD Object” is an option that is not normally used. See the Disjointed Hostnames and AD Objects section of the Intel® SCS User Guide for more information.

By default, all the new objects that the RCS creates are put into the “Domain Computers” security group. If there are additional security groups that the objects should be placed in this can be configured on the AD Integration panel as well.

The Advanced options for AD Integration allow additional attributes to be added to all objects that the RCS creates.

Access Control List Tab

The Access Control List (ACL) configuration is used to specify which AD users or security groups are allowed to access the AMT device with Kerberos. In addition, more digest (username and password) users can be granted access.

The Access Type setting can be set to Local, Remote, or Both. This specifies the location from which the user is allowed to connect and perform an action on the AMT device. Local access is only available on the host itself while Remote access is only available via the network. For ZCentral Connect this should be either Remote or Both.

The Realm setting can be used to allow a user to only perform a subset of actions on the AMT device. “PT Administrator” has access to all realms. For ZCentral Connect to perform correctly it must have access to the PT Administrator realm.

Transport Layer Security Tab

Transport Layer Security is an important configuration option to encrypt AMT traffic between the AMT devices and the system running ZCentral Connect. Choose to "Request certificate from Microsoft CA" and choose the Enterprise Certificate Authority for the enterprise domain that the AMT devices will be living in. Select the certificate template created in the **Create Certificate Template for AMT Server Certificates** section above.

The Common Names of the certificates, both requested and installed, can be customized to fit the need of the enterprise environment. By default, the Subject of the certificate will be the FQDN. By default, the Subject Alternative Name will include the FQDN, Host Name, SAM Account Name, User Principal Name, and the UUI of the AMT device.

If Mutual Authentication (mTLS) is needed check the box next to "Use mutual authentication for remote interface." Then edit the list of trusted root certificates. Add the enterprise CA certificate to the list along with any other root certificates needed to validate client certificates in the environment. Optional advanced settings allow the addition of a certificate revocation list or domain name suffixes. These advanced settings add more requirements for a client certificate to be validated by the AMT device.

System Settings Tab

In the System Settings tab it is important that the Intel® Management Engine is Always On (S0-S5) to enable all features required for ZCentral. Other options can be changed to fix the requirements of specific environments.

The Intel® MEBx Password is set only if the current MEBx password is the default ("admin") otherwise it is not changed. If the password has already been set in MEBx, then this setting will be ignored. Once the password is changed from default, the password must be changed through MEBx.

The AMT default admin user password can be defined in different ways. It can be specified for the profile or use a master password set in RCS. Using a master password allows the password to only be entered once for all profiles. It is also possible to create a random password for each system and rely on only Access Control Lists. Note that using a random password for each system could result in being locked out of a system. Resetting CMOS is the only way to reset a password and this resets AMT provisioning settings to factory settings. The CMOS Reset operation also resets the MEBx password to the default.

For more detailed information on other settings see the **Defining System Settings** section in the Intel® SCS User Guide.

Create script to gather information unavailable from Hello Packets

When Hello Packets are sent to the RCS, they contain all, but two pieces of information needed to complete provisioning. The FQDN of the machine requesting provisioning and the configuration profile to use are still needed. Therefore, when the RCS receives hello packets from an AMT device the following happens:

1. The RCS sets environment variables (on the RCS host) with values sent by the hello packets.
2. The RCS launches an executable that will gather the required information using the environment variables.
3. The executable restarts provisioning with the RCS API's **ConfigAMT** command.
4. The RCS configures the AMT device.

The SCS download package contains an example script which uses WMI to connect to the system and get the FQDN. This example doesn't help in the case where a Windows OS is not running or installed. The example also hardcodes the name of the configuration profile.

If a Windows OS is running on all AMT devices the ACU provisioning method is the best solution. So, for all other cases a custom script will have to be written.

The RCS script collects the following environmental variables:

- CS_AMT_UUID: The UUID of the AMT device
- CS_AMT_ADDRESS: The IP address of the AMT device
- CS_AMT_CONFIGURATION_METHOD: Which type of method is to be used for provisioning. 1 is PSK and 2 is PKI. PSK has been deprecated starting with AMT 9.0.
- CS_AMT_PID: The PID of the PSK key, only used for the PSK method.

The script will be very different depending on the environment and setup steps being taken.

If all AMT devices will be provisioned with the same configuration profile, then it can be hardcoded into the script. If not, logic will have to be built in to use the information in the environmental variables for deciding which profile to use.

If the AMT devices already have a FQDN listed in DNS, then a reverse DNS lookup can be used to associate the IP address. A lookup table between the IP address and the desired FQDN could also be used. Planning is required before starting hello packets to ensure smooth and correct provisioning.

Set RCS Advanced Configuration Options

The RCS has 3 advanced configuration options, only 1 can be used at a time. These options can be changed in the SCS console under Settings.

- None: This is used for the ACU method using default settings.
- One-Time Password required: This option is used to ensure that the source of the provisioning request is the same as the AMT device being provisioned. This is used for the ACU method. If this is selected, then a one-time password (OTP) is required within the provisioning request. The requester (ACU) is responsible for setting the OTP in the AMT device. The RCS will gather this OTP from the AMT device before configuration and ensure that it matches the one from the request. This ensures that the request and the target AMT device are the same machine.
- Support Configuration triggered by Hello messages: This is the option required to support the Hello Packet provisioning method. If this option is selected then the listener port can be specified, by default AMT devices send hello packets to port 9971. The executable (script) path must be provided to select this option. This script is the one talked about in the **Create script to gather information unavailable from Hello Packets** section.

Enable AMT in BIOS Menus

Since Intel® AMT is disabled by default on modern Z Workstations, and therefore the Intel® AMT setting must be enabled prior to AMT provisioning and prior to the AMT network interface to be active. This operation can be done manually by going into the F10 BIOS Menus during POST or it can be performed using the **BIOS Configuration Utility** described above. When in F10 BIOS Menus, navigate to the Advanced Tab, under Remote Management Options, Intel® AMT can be enabled by checking the box next to, “Intel® Active Management Technology (AMT)”.

Ensure Provisioning Certificate is trusted by AMT Device

For enterprise provisioning to work, the AMT device needs to trust the RCS as explained in the **About Provisioning Certificate** section.

If the root certificate, which was used to issue the RCS provisioning certificate, has been pre-installed in ME it will already be trusted by AMT.

If the root certificate, which was used to issue the RCS provisioning certificate, is not a pre-installed certificate then the certificate hash must be added to ME. This can be done via the MEBx menu or by booting to an AMT configuration USB binary file.

Pre-Installed Certificate Hashes in ME v12.0.6:

- VeriSign Universal
- VeriSign Class 3 Primary CA-G1
- VeriSign Class 3 Primary CA-G1.5
- VeriSign Class 3 Primary CA-G2
- VeriSign Class 3 Primary CA-G3
- VeriSign Class 3 Primary CA-G5
- Go Daddy Root CA – G2
- Go Daddy Class 2 CA
- Comodo AAA CA
- Starfield Root CA – G2
- Starfield Class 2 CA
- GTE CyberTrust Global Root
- Baltimore CyberTrust Root
- CyberTrust Global Root
- Verizon Global Root
- Entrust.net CA (2048)
- Entrust Root CA
- Entrust Root CA – G2
- Affirm Trust Premium

Adding Certificate Hash With MEBx

1. Open the MEBx menu by pressing F6 during POST (Note that Intel® AMT must be enabled in BIOS F10 menus to expose MEBx).
2. Login to MEBx.
3. Go to the “Intel® AMT Configuration” menu.
4. Go to “Remote Setup And Configuration”⟶“TLS PKI”⟶“Manage Hashes”.
5. Press the “Insert” key to enter a new hash.
6. When prompted, enter the name of the Hash (only used to find it) and press the “Enter” key.
7. When prompted, enter the hash and press the “Enter” key.
8. Press the “Y” key to set the hash as active.

Adding Certificate Hash With USB

The AMT SDK provides a USBFile.exe utility which can be used to insert hashes into ME by booting to the USB. The utility is located in the directory, **\AMT_SDK_12.0.0.9\Windows\Intel_AMT\Bin\Configuration\USBFile\**. The readme for the utility is located in the directory, **\AMT_SDK_12.0.0.9\Windows\Intel_AMT\Samples\Configuration\USBFile\.**

Boot to OS

The ACU application must be run on a Windows OS. The following are also required:

- The HECI driver (also called the Intel® Management Engine Interface (MEI) driver) must be installed and preferably up to date
- The Intel® Local Manageability Software (LMS) service must be running
- The OS must have WMI enabled

Request Provisioning

To initiate provisioning with the ACU method the ACU application must be run from the Windows OS of the AMT device. For detailed information about the AMT Configuration Utility see Chapter 6 of the Intel® SCS User Guide.

The ACU is a standalone executable, ACUConfig.exe. The SCS download package contains the installer for the ACU. After installation it can be found by default at “C:\Program Files (X86)\Intel\SCS ACUConfig\ACUConfig.exe”. The ACU is used via its Command Line Interface (CLI). The ACU must be run with administrator privileges.

The ACU will put all output, by default, into a log file (“ACUlog_HostName_YYY-MM-DD-HH-MI-SS.Log”) where ACUConfig.exe is located. To view the output in the terminal, specify /Output Console as a command line parameter. Verbose output can be enabled by specifying /Verbose as a command line parameter.

The account running the ACU should have WMI permissions on the RCS host. If it does not, credentials for an account that does have WMI permissions on the RCS host will need to be entered as command line arguments.

To start enterprise provisioning the ACU command needed is **ConfigViaRCSOnly, using the following syntax**:

ACUConfig.exe [options] ConfigViaRCSOnly <RCS Network Address> <Configuration Profile Name> [/WMIUser <username>] [/WMIUserPassword <password>] [/AdminPassword <password>] [/NetworkSettingsFile <file>] [/AbortOnFailure] [/ADOU <path>] [/RCSBusyRetryCount <retries>]

- RCS Network Address: FQDN or IP address for the RCS host
- Configuration Profile Name: Name of the profile created in the Intel® SCS console
- WMIUser: Username (domain\username format) of a domain account with WMI permissions on the RCS host
- WMIUserPassword: Password of the WMIUser
- AdminPassword: Current digest admin password (This is not required if the AMT device is unconfigured/unprovisioned)
- NetworkSettingsFile: Path to a file with network settings used to configure the AMT device
- AbortOnFailure: Causes the AMT device to be put back into the “Not Provisioned” state if configuration fails at any point
- ADOU: Path to the AD OU that contains the provisioned objects (Only used if reprovisioning, will delete the old object before adding a new one)
- RCSBusyRetryCount: The number of times to retry the configuration request if the RCS responds with a busy status (Default: 0)

Example:
ACUConfig.exe /Verbose /Output Console ConfigViaRCSOnly IntelRCSServer.domain.local “Main Configuration”.

Enable Hello Packets

Hello Packets can be enabled from the MEBx Menu. When they are enabled, the AMT device will start sending hello packets to the host “ProvisionServer” resolved by DNS or to the IP address/FQDN defined in MEBx. Once enabled the Hello Packets will stop being sent after a set period of time (usually 12 hours). They can be re-enabled manually through the same means.

When hello packets are received by the RCS, they are handled as described in the **Create script to gather information unavailable from Hello Packets** section.

To enable Hello Packets in MEBx first open the MEBx menu by pressing F6 during POST. Login to MEBx and go to the “Intel® AMT Configuration” menu. Go to “Remote Setup and Configuration” then “RCFG” and then select “Start Configuration”. Hit the “Y” key when prompted to start remote configuration. Hello packets will start to be sent periodically until the system has been provisioned.

A USB based provisioning file can also be used to enable the RCFG setting by booting to the USB key. This can be done without performing full provisioning through USB.

The ACU can also be used to send a Hello Packet to the RCS, **using the following syntax**:

ACUConfig.exe [options] SendHello <RCS Network Address> [<RCS Network Port>]

Note that the ACU can only be used in a Windows OS even when only being used to send a Hello Packet.

AUTOMATING THE PROCESS

Once the one-time setup is complete it would be best if each new device needing to be provisioned didn't have to be physically accessed. There are different ways that this can be accomplished and depends on the enterprise environment and setup process. These are some examples of options available.

Intel® SCS add-on for SCCM

Intel® provides an add on for Microsoft's System Center Configuration Manager (SCCM) that can assist in the discovery and provisioning of AMT devices. The add on requires a profile to be created in SCS before being installed. The add on will create collections, deployments, packages, and task sequences in SCCM. After a new machine is added to the network controlled by SCCM it can be discovered by the Discovery task sequence and placed in a collection that marks it as AMT Enabled. Then a configuration task sequence can be run on all machines in that collection which will deploy a package to all the machines that contain a script and the ACU. The script will execute the ACU on each machine to request provisioning from the RCS server.

As with the ACU, SCCM clients only run on Windows and the ACU requirements still apply. The only step that this automates by default is **Request Provisioning**.

The add-on provides base functionality and example task sequences. However, these base blocks can be used to create a custom automated process that fits different environments. Using PXE boot and custom WinPE OS images can be used as well to help with the process.

Using HP Custom Services

The HP Custom Services team can pre-provision systems using the manual provisioning process, such that when you receive the system you immediately have AMT access when you connect to your network.

What the HP Custom Services team can do is enable AMT in BIOS, set a defined MEBx password, enable network access, load custom certificate hashes, and set static network settings (IP and DNS). These services are not offered in the standard configure to order factory process and must be requested through your HP sales rep. When requesting this service be prepared to provide the required information such as MEBx passwords and other provisioning information specific to your AMT environment.

CONTACT US

4AA7-7256ENW, April 2020.