Intel® Endpoint Management Assistant (Intel® EMA)

Configuring LAN-less Endpoints to ACM

Intel® EMA Version: 1.3 and later

Document update date: Friday, March 12, 2021

Legal Disclaimer

1 Introduction

Intel® Endpoint Management Assistant (Intel® EMA) is a software application that provides an easy way to manage Intel vPro® platform-based devices in the cloud, both inside and outside the firewall. Intel EMA is designed to make Intel® AMT easy to configure and use so that IT can manage devices equipped with Intel vPro platform technology without disrupting workflow. This in turn simplifies client management and can help reduce management costs for IT organizations.

Intel EMA and its management console offer IT a sophisticated and flexible management solution by providing the ability to remotely and securely connect Intel AMT devices over the cloud. Benefits include:

- Intel EMA can configure and use Intel AMT on Intel vPro platforms for out-of-band, hardware-level management
- Intel EMA can manage systems using its software-based agent, while the OS is running, on non-Intel vPro® platforms or on Intel vPro® platforms where Intel AMT is not activated
- Intel EMA can be installed on premises or in the cloud
- You can use Intel EMA's built-in user interface or call Intel EMA functionality from APIs

This document provides specific information to configure LAN-less endpoints in Admin Control Mode (ACM) using either Intel EMA or Intel SCS. It does not provide complete installation and usage instructions for either of these tools. This document is intended as a supplemental companion piece to the complete set of product documentation for Intel EMA and/or Intel SCS.

For complete installation, setup, and configuration instructions for Intel EMA, including recommended security settings, see the *Intel® EMA Single Server Installation and Maintenance Guide*, the *Intel® EMA Distributed Server Installation and Maintenance Guide*, and the *Intel® EMA Administration and Usage Guide*.

Intel EMA documentation:

https://www.intel.com/content/www/us/en/support/products/123804/software/manageability-products/intel-endpoint-management-assistant-intel-ema.html

Documents are under both **Product Information & Documentation** and **Install & Setup** links.

Intel SCS documentation:

https://www.intel.com/content/dam/support/us/en/documents/software/Intel_SCS_User_Guide.pdf

Intel AMT documentation:

For additional information about Intel AMT, please see the following documentation:

https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm

2 Setting or Verifying the Correct PKI DNS Suffix in Intel® MEBX

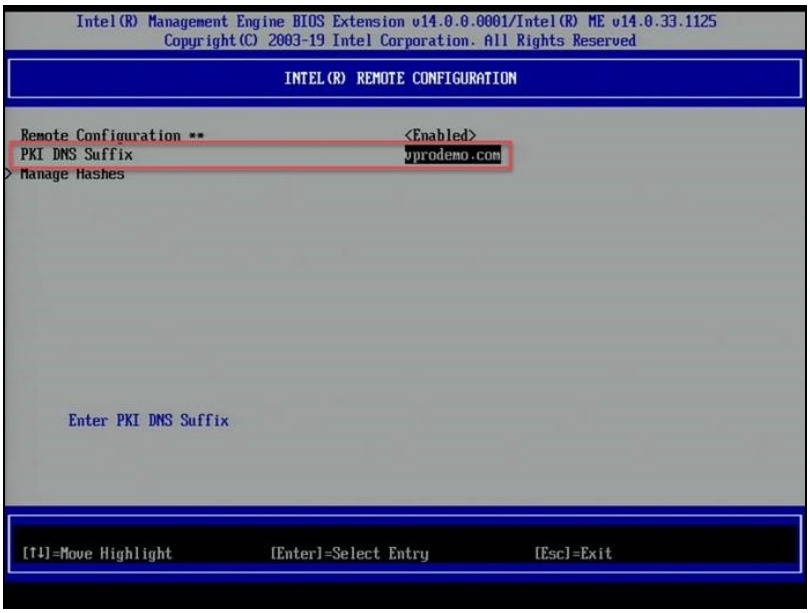
This procedure is required in order to configure Intel AMT in Admin Control Mode (ACM) on LAN-less endpoints. For LAN-less devices, there currently is no way for Intel AMT to determine that it is on the same domain as the PKI certificate's DNS suffix. Therefore, in order to configure a LAN-less endpoint's Intel AMT in ACM, you must first manually add the PKI certificate's DNS suffix to the LAN-less endpoint's Intel MEBX, as described below.

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

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

1. Restart the LAN-less endpoint and press **Ctrl-P** during startup.
2. Select **Intel MEBX Login** and enter the Intel MEBX password.
3. Select **Intel(R) AMT Configuration > Remote Setup and Configuration > TLS PKI > PKI DNS Suffix**, to reach the screen shown below. Note that this menu choice is only available if Intel AMT has not been provisioned on this device.
4. Verify or set the PKI DNS Suffix value to ensure it matches the PKI certificate's domain suffix value.

Figure 1: Intel MEBX PKI DNS Suffix Configuration



Note: Intel EMA performs a full unprovision of Intel AMT and deletes any custom root certificate hashes and the PKI DNS suffix from the Intel AMT settings. As such, if you unprovision a system on a remote network and then want to reprovision that system using Admin Control Mode, you may need to physically touch that system in order to do that.

3 Configuring LAN-less Endpoints with Intel® EMA

This section describes how to configure LAN-less endpoints using Intel EMA.

1. Review the Intel AMT setup flow in Intel EMA (section 3.1).
2. Manually update the PKI DNS suffix in Intel MEBX on the LAN-less system (section 2).
3. Use Intel EMA to upload an Intel AMT PKI certificate (section 3.2).
4. Either auto-provision your enpoints (section 3.3), or manually provision endpoints individually (section 3.4).

Note: These instructions assume you have a working installation of Intel EMA and are familiar with the installation, configuration, and usage instructions in the Intel EMA product documentation.

3.1 Intel® AMT Provisioning/Setup Flow in Intel® EMA

This section describes what happens programmatically when you either enable auto-setup of Intel® AMT for your managed endpoint systems (section 3.3), or manually perform an on-demand setup of Intel AMT (section 3.4).

Note: Intel® AMT setup is also known as provisioning.

Intel® EMA uses **Host Based Configuration (HBC)** to provision Intel AMT on your endpoints. HBC is performed in-band via the endpoint's operating system. If you do not upload a Public Key Infrastructure (PKI) certificate, Intel EMA sets Intel AMT to Client Control Mode (CCM) on the endpoints. There are limitations when using CCM, such as requiring user consent at each endpoint in order to perform some of Intel EMA's remote connection capabilities. Uploading a PKI certificate enables Intel EMA to set the endpoint's Intel AMT into Admin Control Mode (ACM). LAN-less endpoints require a manual Intel MEBX update (see Round 1 below). The added security of the PKI certificate and ACM allows Intel EMA to connect to the endpoint's Intel AMT and perform remote actions without user consent.

Note: Refer to Intel AMT documentation for more information about Host Based Configuration, Client Control Mode, and Admin Control Mode. https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm

The provision/setup is divided into 2 rounds.

1. **Round 1:** Sets the endpoint into Client Control Mode. Then, if you have uploaded a PKI certificate and selected TLS-PKI as setup method in your Intel AMT auto-setup, Intel EMA brings the endpoint from Client Control Mode to Admin Control Mode.

   Note: For LAN-less endpoints, you must first manually update the endpoint's Intel MEBX to add the uploaded PKI certificate's DNS suffix in order for Intel EMA to bring the endpoint from Client Control Mode to Admin Control Mode. Otherwise the endpoint will remain in CCM. See section 2 for details.

2. **Round 2:** After round 1 is complete (i.e., Intel AMT is successfully provisioned, either in CCM or ACM), Intel® EMA configures other Intel AMT settings such as power policy, KVM interface, CIRA, etc.

If round 1 fails, Intel EMA will un-provision the endpoint, then automatically retry the provision/setup every three minutes until it is successful or until one hour passes without success.

If round 2 fails, Intel EMA will keep the endpoint provisioned and continue trying the round 2 setup every three minutes until it is successful or one hour passes without success.

3.2 Upload Intel® AMT PKI Certificates

Intel® AMT PKI certificates are required if you want to provision Intel AMT on your endpoints in Admin Control Mode (ACM), which allows remote connection without user consent. Without a PKI certificate, Intel® EMA provisions Intel® AMT in Client Control Mode (CCM), which requires user consent for remote operations on each endpoint.

The certificate must be a valid Intel AMT PKI certificate with the correct OID or OU indicating that it is an Intel AMT PKI certificate. Intel EMA does not validate the certificate information. However, if the certificate values are incorrect for the domain in which the provisioning process is running, provisioning will fail.

Notes:

- Refer to Intel AMT documentation for more information on ACM and CCM, and to find the requirements and the process to obtain a valid Intel AMT PKI certificate.
- In Intel ME 11.0 the default SHA1 certificate hashes were removed from the firmware. Hashes could still be added in manufacturing, or through the Intel MEBX or WS-MAN commands.
- Starting with Intel ME 15.0 firmware for desktops, and Intel ME 16.0 firmware for all platforms, Intel is removing support of SHA1 root certificates and RSA key sizes smaller than 2048 bits for Intel AMT provisioning. In those releases and later, it is no longer possible to add SHA1 hashes.
- For expiring certificates, you must upload a new certificate and enter a new **Entry Name** and **Password**. Do not re-use the **Entry Name** for the existing, expiring certificate when uploading the new certificate. You will need to update any Endpoint Group configurations that use the expiring certificate with the new certificate's **Entry Name**.
- If you have installed the Intel EMA Server on a machine running Windows Server 2012 or 2016 (earlier than build 1709), uploading a certificate into Intel EMA will fail if the certificate PFX file used encryption “AES256-SHA256". An error about an invalid password will be displayed, even though a valid password is provided.

  See Troubleshooting in the *Intel® EMA Administration and Usage Guide* for information on how to accommodate this.

The certificate is stored in the Intel EMA database and loaded into memory for optimal performance. If an updated certificate file (which includes any of the certificates in the certificate chain) is re-uploaded with a change, it may take up to 15 minutes for the change to be processed and reflected for usage.

You can upload multiple certificates for a given Tenant, and you can upload the same certificate to multiple Tenants. However, each Endpoint Group in a given Tenant can only have one PKI certificate associated with it.

To upload a certificate:

1. From the navigation pane at left, click **Settings**, then select **Server Settings > Certificates**. A list of certificates available for use is displayed. Intel AMT PKI certificates are designated by a blue “PKI Certificate” label. Others are the root certificates used by the PKI certificates.
2. Click **Upload**.
3. The Certificate dialog is displayed. If the certificate to be uploaded is not an Intel AMT PKI certificate, uncheck the **PKI certificate** checkbox.
4. Enter the **Entry Name** and **Password**, then click **Choose File**. Note that the certificate file to be uploaded must be less than 1MB. If you are uploading a PKI certificate file, the file should include the full certificate chain, including the Private Key. Do not re-use an **Entry Name** that you are already using.
5. In the Certificate dialog, click **Upload**.

You can also download and delete certificates. Note that if the certificate is still used by another certificate (in the certificate chain), or if it is used in an Intel AMT Profile or Intel AMT setup, it cannot be deleted.

3.3 Enable Intel® AMT Auto-Setup

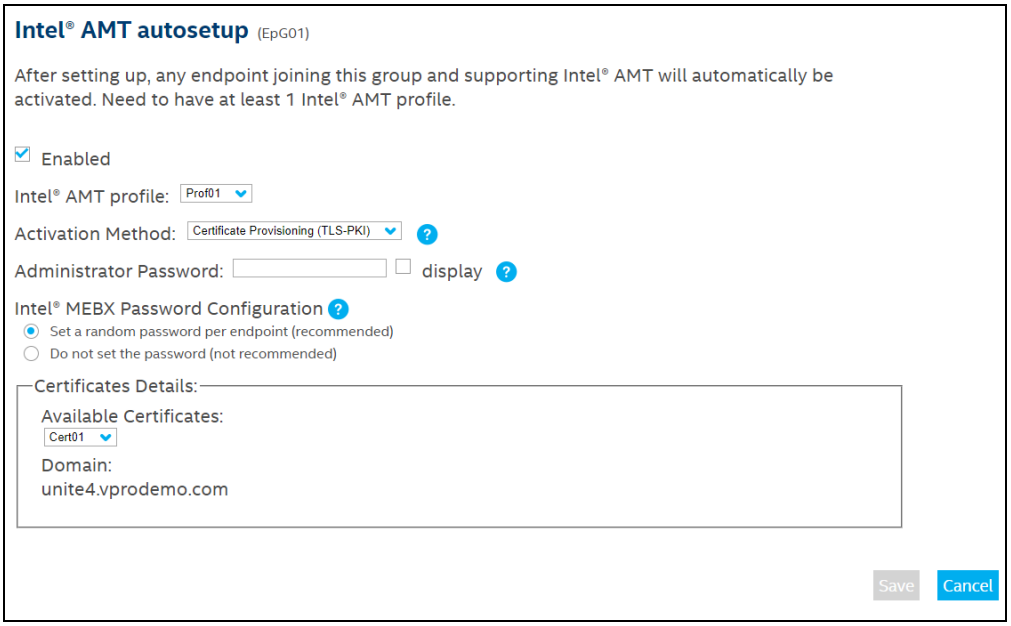
Note: Intel® AMT setup is also called Intel AMT provisioning.

Intel AMT auto-setup can be enabled or disabled for each endpoint group. If it is enabled, Intel EMA will try to set up all endpoints that register in this endpoint group. This setup is triggered when an endpoint disconnects and then reconnects to the Intel EMA server, or when an agend first connects if the Intel AMT auto-setup was defined before deploying the agent.

To enable auto-setup:

1. From the navigation bar at left, select **Endpoint Groups**, then click the ellipsis (**...**) next to the target endpoint group and select **View Configuration**.
2. On the configuration page for that endpoint group, click **Intel® AMT Autosetup**.
3. Select the **Enabled** checkbox and choose the **Intel® AMT profile** you created previously.
4. Select the **Activation Method** to be used. The TLS-PKI activation method will appear only when there is at least one valid Intel AMT PKI certificate for this tenant. A Tenant Administrator can use the Settings page to manage the available PKI certificates (Section 3.2). See Sections 1 and 3.1 for more details about the activation methods.
5. Enter the **Administrator Password**. The administrator password you enter will be set as the password for the "admin" account in Intel AMT on the endpoint system.
6. Choose whether or not to set a random password for the Intel® Management Engine BIOS Extension (Intel® MEBX) on the endpoints configured with this Intel AMT profile. We recommend that you have Intel EMA set a random Intel MEBX password on your endpoints. If necessary, you can retrieve the random password for an endpoint using the Intel EMA API. See the *Intel® EMA API Guide* for more information.
7. Select a certificate from **Available Certificates** (if any are available).
8. Click **Save**.

Figure 2: Intel AMT Autosetup screen



If the configuration in the auto-setup is changed (i.e., the Intel® AMT profile is changed), Intel® EMA will try to apply these changes almost immediately to all endpoints that are in-band-connected. For the endpoints that are not connected, the changes will be applied when they reconnect to the Intel® EMA server.

However, if either the certificate or the activation method (i.e., host-based or TLS-PKI) is changed, then Intel® EMA cannot apply such changes automatically. You will need to unprovision the endpoint(s) first.

3.4 Intel® AMT On-demand Setup

Intel® AMT setup is also called Intel AMT provision.

You can perform an Intel AMT setup/cleanup action in an on-demand way, at a single endpoint. However, the Intel AMT profile cannot not be used in the on-demand setup. The dropdown Intel AMT profile menu is disabled. The on-demand setup will perform very basic configurations. See Section 3.1 for more details.

To access this page, open the action dropdown menu for an endpoint, and then choose "Provision Intel® AMT." This option is enabled only if the target endpoint is Intel AMT capable. Then you can use this page to provision or unprovision Intel AMT.

About the activation methods:

- The TLS-PKI activation method will appear when there is at least one valid Intel AMT PKI certificate for this tenant. A Tenant Administrator can use Settings page to manage the available PKI certificates. See Section 3.2 for more details.
- Intel EMA still uses a host-based flow to set up Intel AMT, even when TLS-PKI is chosen.

The Administrator Password you entered will be set as the password for the admin account in Intel AMT.

Choose whether or not to set a random password for the Intel® Management Engine BIOS Extension (Intel® MEBX) on the endpoints (only available for PKI provisioning). We recommend that you have Intel EMA set a random Intel MEBX password on your endpoints. If necessary, you can retrieve the random password for an endpoint using the Intel EMA API. See the *Intel® EMA API Guide* for more information.

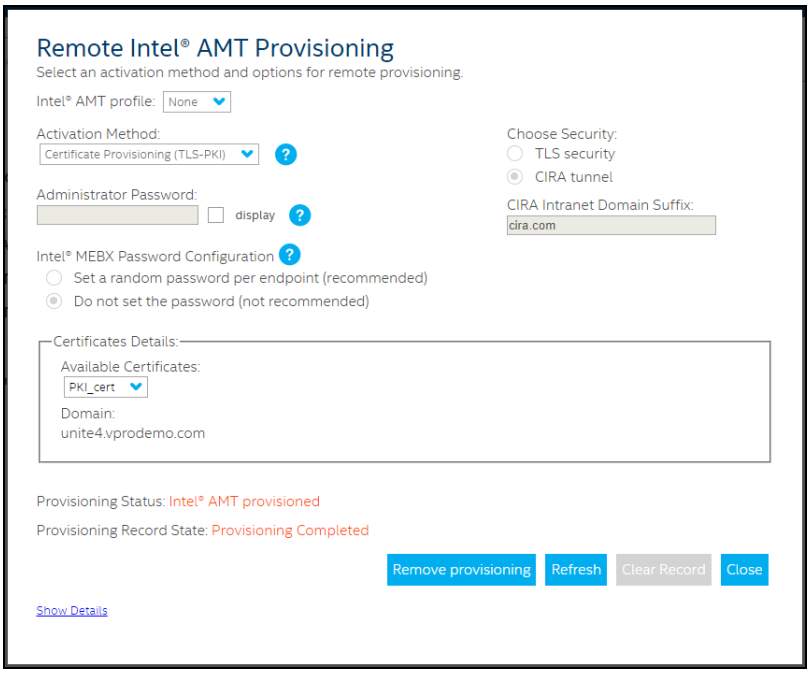
Note: If you unprovision the endpoint the random Intel MEBX password will be deleted from the Intel EMA database, and thus not retrievable by the API. Before unprovisioning an endpoint, be sure to retrieve its Intel MEBX password and note it down. This is particularly important for LAN-less systems, as you may need to reset the PKI DNS suffix in the Intel MEBX prior to reprovisioning. See section2 for more information on LAN-less systems.

Provision Status: This is the provision status of the target Intel AMT.

Provision Record State: This is the current setup/cleanup action status. Intel EMA maintains a setup/provision record for each Intel AMT setup. This record indicates the setup status of the endpoint. If the setup/provision process fails, Intel EMA will pick up this record again and retry it periodically. Therefore, when the setup/provision process is in progress, you will see a button to "Clear Record." If the record is cleared, Intel EMA will not attempt any further provisioning operations.

The setup of the target Intel AMT is complete when Provision Status is "Provisioned" and the Provision Record state is "Complete".

Figure 3: Provision Intel® AMT on-demand



4 Configuring LAN-less Endpoints with Intel® SCS

This section describes how to configure LAN-less endpoints using Intel SCS.

Note: These instructions assume you have a working installation of Intel SCS and are familiar with the installation, configuration, and usage instructions in the Intel SCS product documentation.

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

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

The procedure below describes how you can configure LAN-less systems in Admin Control mode.

1. Make sure that the correct PKI DNS Suffix for your organization is defined in the Intel MEBX. Remote configuration of these systems requires that this value be pre-defined in the Intel MEBX by the manufacturer/supplier of the Intel AMT system. If it was not pre-defined, you can add it manually in the Intel MEBX. See section 2.
2. Configure the system locally into Client Control mode.
3. Use the MoveToACM command to move the system to Admin Control mode. See Remote Configuration of LAN-less Systems (section 4.1).

Although these are the only steps required, it is recommended to configure only basic settings in step #1. Then, after step #2, remotely configure all the remaining required settings. For the recommended procedure, see Remote Configuration of LAN-less Systems (section 4.1).

Note: When unconfiguring these systems, do NOT use the /Full parameter or the Full Unconfiguration job operation type. Full unconfiguration will delete the PKI DNS Suffix value.

4.1 Remote Configuration of LAN-less Systems

1. In the Intel SCS Console, create two profiles specifically for LAN-less systems:

   A “basic” profile — This profile will be used for local configuration to Client Control mode. These are the only settings that are required in the basic profile:

   - In the Optional Settings window, select the WiFi Connection check box and define a WiFi Setup.

     (Without this WiFi Setup, remote connection to Intel AMT will not be possible after configuration.)
   - In the System Settings window, leave the default settings. But when defining the password for the Intel AMT admin user, make sure that you select only the option named “Use the following password for all systems”. Make sure that you define a strong password.
   - A “full” profile — This profile will be used to reconfigure the system with all the settings you want to configure in Intel AMT. Make sure that this profile also includes a WiFi Setup.

2. Select the “basic” profile and then click Export to XML to export the profile to an XML file. Make sure that you do NOT select the check box named “Put locally configured devices in Admin Control mode”.
3. Use the ConfigAMT command of the Configurator to configure the system using the exported XML file. For example:

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

   After the command has completed successfully, Intel AMT will be configured in Client Control mode.
4. Use the MoveToACM command of the Configurator to move the system to Admin Control mode (see Moving from Client Control to Admin Control in the Intel SCS Users Guide). For example:

   ```
   ACUConfig.exe MoveToACM 192.168.1.10
   ```

   After the command has completed successfully, Intel AMT will be configured in Admin Control mode.
5. Use the ConfigViaRCSOnly command of the Configurator to reconfigure the system using the “full” profile (see Configuring Systems using the RCS in the SCS Users Guide). For example:

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

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