# Intel® Endpoint Management Assistant (Intel® EMA)

## Administration and Usage Guide

***Rev. 1.15.1***

***October 2026***

Doc. No.: , Rev.: 1.15.1

# Legal Disclaimer

Copyright 2018-2026 Intel Corporation.

This software and the related documents are Intel copyrighted materials, and your use of them is governed by the express license under which they were provided to you ("License"). Unless the License provides otherwise, you may not use, modify, copy, publish, distribute, disclose or transmit this software or the related documents without Intel's prior written permission.

This software and the related documents are provided as is, with no express or implied warranties, other than those that are expressly stated in the License.

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.

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 computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses. Check with your system manufacturer or retailer or learn more at

http://www.intel.com/technology/vpro.

Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

# Contents

**Legal Disclaimer** ..... **2**
**Revision History** ..... **8**

**1.0 Introduction** ..... **9**
1.1 Usage Requirements ..... 9
1.1.1 Agent Prerequisites ..... 10
1.2 Key Concepts ..... 11
1.2.1 Tenant ..... 11
1.2.2 User Roles ..... 11
1.2.3 Endpoint Groups ..... 12
1.2.4 User Groups ..... 12
1.2.5 Intel® EMA Agent ..... 14
1.2.6 In-band vs. Out-of-band ..... 15
1.2.7 Intel® AMT Provisioning/Setup Flow in Intel® EMA ..... 16
1.2.8 USB Redirection ..... 18
1.2.9 Remote Secure Erase ..... 19
1.2.10 Intel® Remote Platform Erase Overview ..... 20
1.2.11 One Click Recovery ..... 20
1.2.12 Microsoft Entra ID Authentication ..... 21
1.2.13 Intel LMS Features and Installation ..... 22
1.2.14 Important File and Directory Locations ..... 23

**2.0 Logging in to Intel® EMA** ..... **24**
2.1 Overview Page ..... 25
2.1.1 Adding or Removing Server Name from Footer ..... 25
2.2 Setting up Two Factor Authentication ..... 26

**3.0 Setting Up Your Tenant(s)** ..... **29**
3.1 Create Your Endpoint Groups ..... 30
3.1.1 Creating New Endpoint Groups ..... 31
3.1.2 Viewing and Deleting an Endpoint Group ..... 32
3.2 Create Agent Files for Deployment to Managed Endpoints ..... 33
3.3 Create Your Network Profiles ..... 34
3.3.1 Creating a New Wi-Fi Profile ..... 35
3.3.2 Creating a New 802.1x Profile ..... 36
3.4 Create Your Intel AMT Profiles ..... 38
3.4.1 General Settings ..... 39
3.4.2 Power State Settings ..... 40
3.4.3 Management Interface Settings ..... 40
3.4.4 FQDN Settings ..... 41
3.4.5 IP Address Settings ..... 42
3.4.6 Wi-Fi Settings ..... 42
3.4.7 Wired 802.1x Settings ..... 43
3.5 Upload Certificates ..... 43
3.5.1 Upload Intel® AMT PKI Certificates ..... 44
3.5.2 Setting or Verifying the Correct PKI DNS Suffix in Intel® MEBX ..... 45
3.6 Enable Intel AMT Auto-Setup ..... 46

**4.0 Deploying the Agent to Your Endpoints....49**
4.1 Install Directory....50
4.2 Intel® EMA Agent Database....50
4.3 Windows Service Information....50
4.4 Proxy Configuration....51
4.5 Verifying and Troubleshooting Agent Installation....51

**5.0 Managing Users and User Groups....55**
5.1 Adding, Modifying, and Deleting Users....55
5.2 Creating New User Groups....56
5.3 Assigning Endpoint Groups to User Groups....57
5.4 Managing Active Directory User Groups....57
5.5 Managing SAML Authentication Users....58

**6.0 Managing Your Endpoints....59**
6.1 Intel® AMT On-demand Setup....59
6.2 Intel® EMA Agent....60
6.2.1 Agent Windows Registry Information....61
6.3 Viewing Your Endpoints....61
6.3.1 General Tab....62
6.3.2 Hardware Manageability Tab....62
6.3.3 Desktop Tab....63
6.3.4 Terminal Tab....65
6.3.5 Files Tab....66
6.3.6 Processes Tab....66
6.3.7 WMI Tab....66
6.4 Performing Actions on Endpoints....66
6.4.1 Wake....67
6.4.2 Set Alarm Clock....67
6.4.3 Sleep/Hibernate/Power off/Restart....68
6.4.4 Send Alert....68
6.4.5 Remote File Search....68
6.4.6 Stop Managing an Endpoint....68
6.4.7 Provision Intel® AMT....69
6.4.8 View Desktops....69
6.4.9 Mount an Image....70
6.4.10 Boot to Recovery Image....71
6.4.11 Platform Erase....72

**7.0 Managing Disk Images....74**
7.1 Uploading Image Files....74
7.2 Editing and Deleting Stored Image Files....75
7.3 Viewing and Managing Active Sessions....75
7.4 Image Recommendations....75

**8.0 Appendix: Troubleshooting....77**

**9.0 Appendix - Modifying Component Server Settings....81**
9.1 Swarm Server....81
9.2 Ajax Server....82
9.3 Manageability Server....83
9.4 Web Server....85

9.5 Security Settings..... 87
9.6 Recovery Server Settings..... 90

**10.0 Appendix - Intel® EMA Agent Console..... 91**

10.1 Files..... 91
10.2 Intel® EMA Agent Database..... 92
10.3 Proxy Configuration..... 92
10.4 Resource Consumption..... 92
10.5 Agent Windows Registry Information..... 93

**11.0 Appendix - Performing Intel® EMA Endpoint Operations from a Machine-to-Machine Client Application..... 95**

11.1 Creating a New Client Credentials Account..... 95
11.2 API Privileges for Client Credentials Account Scopes..... 96
11.3 Requesting a Token Using Client Credentials..... 96

## Figures

1 Intel® EMA Server and Tenants..... 11
2 Relationship between Users, User Groups, and Endpoint Groups..... 13
3 Tenant Administrator Overview.....25
4 Endpoint Group Setup page..... 32
5 Generate Agent Installation Files ..... 33
6 Network Profiles and Intel® AMT Profiles.....34
7 Intel MEBX PKI DNS Suffix Configuration..... 46
8 Provision Intel® AMT On-demand.....60
9 Multi-desktop Viewing..... 70

# Tables

1 Intel® EMA Agent Files..... 49

# Revision History

| Revision Number | Description | Release Date |
|---|---|---|
| 1.14.0 | • **Updated** Microsoft Entra ID Authentication on page 21<br>• **Added** Note related to auto-setup profile on an endpoint already provisioned in CCM systems in Enable Intel AMT Auto-Setup on page 46 | August 2024 |
| 1.14.2 | • Removed the Location Information from the Messaging and Alerts in Create Your Endpoint Groups on page 30<br>• Updated the first note to include the Entra ID credentials in Managing Active Directory User Groups on page 57<br>• Updated Appendix: Troubleshooting on page 77 | February 2025 |
| 1.14.3 | • Updated the db name in Install Directory on page 50<br>• Updated the third sub-bullet of point 5 in To Create a New 802.1X Profile: on page 36 | May 2025 |
| 1.14.4 | • Updated Point two and Note in Logging in to Intel® EMA on page 24<br>• Updated Note point 5 in Adding, Modifying, and Deleting Users on page 55<br>• Updated table in Appendix: Troubleshooting on page 77 | September 2025 |
| 1.14.5 | • Updated Roles in Enable Intel AMT Auto-Setup on page 46 | February 2026 |
| 1.15.0 | • Revision update only | June 2026 |
| 1.15.1 | • Revision update only | October 2026 |

# 1.0 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 describes how set up and configure Intel® EMA to manage your endpoints, once Intel® EMA server installation is complete. It also describes how to maintain and modify your Intel® EMA usage environment (referred to as a Tenant; refer to Chapter 1 below) as your organization grows and changes over time. Further, it defines key concepts and terminology for using Intel® EMA, including which user roles can perform which tasks within the Intel® EMA Tenant environment. Lastly, it presents the management actions you can perform on your managed endpoints, and gives step-by-step instructions for performing those actions.

## 1.1 Usage Requirements

The following components are required in order to use Intel® EMA to manage your endpoints:

- Supported web browsers: Chrome* 63+ (starting from December 2017), Firefox* 52+ (starting from March 2017).
- Knowledge of Intel® Active Management Technology (Intel® AMT): You must possess general knowledge of the Intel AMT solution. You should know appropriate setup/provision approaches and various control modes. Intel® EMA only supports Intel® AMT 11.8.79 or later.

**NOTE**

Intel AMT knowledge is required only if you plan to use Out-of-Band features. (refer In-band vs. Out-of-band on page 15

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

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

### 1.1.1 Agent Prerequisites

**NOTE**

The Intel® EMA Agent is not designed to run in a VM on the target endpoint, even on the Base Hypervisor. The LAN/WLAN cannot interpret multiple IP addresses correctly. No Hypervisor has been written to accommodate the address translation required to use Intel AMT. This affects the agent's ability to connect to Intel AMT and perform Out of Band (OOB) actions on the endpoint. It is possible that in-band actions may work in this scenario, but that is not certain.

This is a list of the prerequisites needed to set up the Intel® EMA Agent:

- **Operating System:** Intel® EMA Agent is officially supported on Microsoft Windows 10 and Windows 11, 64bit operating systems. The 32bit agent has been deprecated and will no longer be released. Systems running the 32bit agent should be updated (a manual update procedure).
- **Firewall:** When Intel® EMA Agent is installed, it will set up the following Windows Firewall in-bound rules for the installed agent binary process. If you are using a different firewall, make sure that the following in-bound rules are set for the installed agent binary process:
  - Peer-to-peer traffic: UDP with local port at 16990, any IP for local and remote addresses, and edge traversal blocked.
  - Peer-to-peer traffic: TCP with local port at 16990, any IP for local and remote addresses, and edge traversal blocked.
  - Local loopback management traffic: TCP with local port at 16991, 127.0.0.1 for local and remote addresses, and edge traversal blocked.
- Intel® Active Management Technology (Intel® AMT): Intel® EMA only supports Intel® AMT 11.8.79 or later Only required for Out-of-band endpoint management. Refer In-band vs. Out-of-band on page 15

  The following table lists the minimum Intel AMT versions required on endpoints to use USBR over CIRA.

| Intel AMT Version | Build Number |
|---|---|
| Intel AMT 11 | 11.8.79 or later |
| Intel AMT 12 | 12.0.70.1607 or later |
| Intel AMT 14 1 | 4.0.45.1341 or later |
| Intel AMT 15 | all |
| Intel AMT 16 | all |

For more information about USBR, refer USB Redirection on page 18.

## 1.2 Key Concepts

The following sections describe the primary tools, components, roles, and processes used in the Intel® EMA solution.

### 1.2.1 Tenant

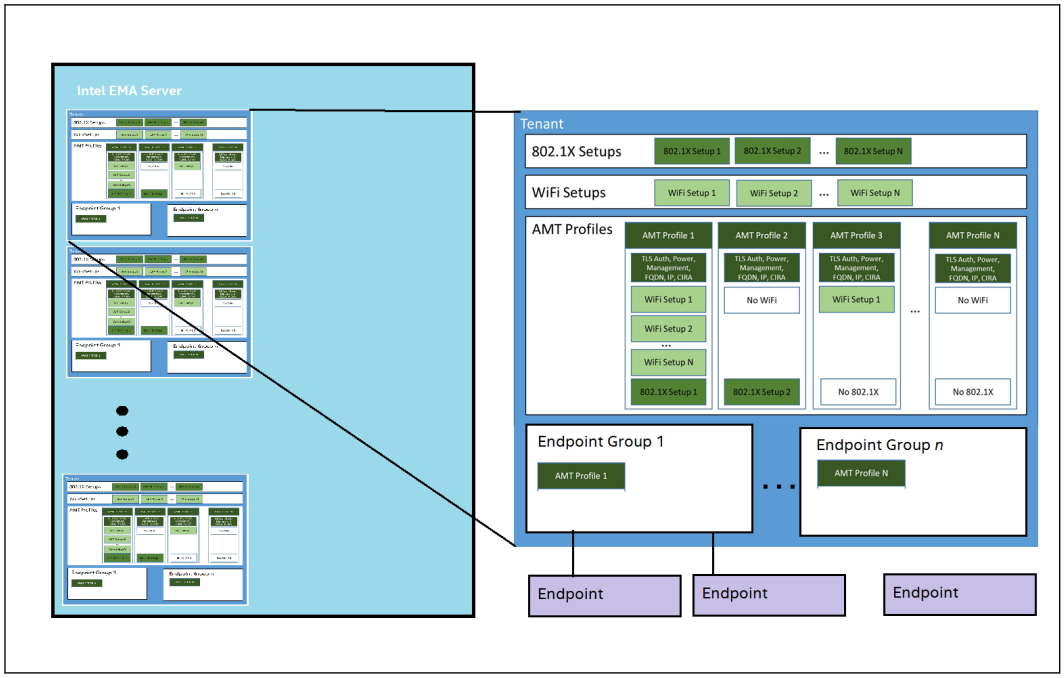
A tenant is a usage space within the Intel® EMA server that represents a business entity. For example, a tenant can be a company, or it can be an organization or office location within a company. One Intel® EMA server can support multiple tenants. The users, endpoint groups, and endpoints under a tenant are separate from those under another tenant.

**NOTE**

The Intel® EMA installer does not create a Tenant Administrator user for the initial Tenant, so you must use the Global Administrator user to create a Tenant Administrator user before proceeding Tenant setup after installation.

The figure below illustrates the relationship between an Intel® EMA server and its Tenants. Other concepts like endpoint groups, profiles, and endpoints are described in subsequent sections.

**Figure 1. Intel® EMA Server and Tenants**




### 1.2.2 User Roles

A user can have only one role. A role, however, can be performed by multiple users. These are the available roles:

- **Global Administrator:** This role performs user management, tenant management, and server management. The Global Administrator does not perform endpoint management and does not (and cannot) belong to any endpoint group. The Global Administrator's control spans all tenants in a single Intel® EMA server installation instance.Tenant Administrator: This role is specific to a particular tenant and can perform all operations (user management, endpoint management) under that tenant. Therefore, the Tenant Administrator does not (and cannot) belong to any user group in its tenant. A
- **Tenant Administrator:** user cannot manage a Global Administrator user.
- **Account Manager:** This role is specific to a particular tenant, and can perform user management only. However, an Account Manager cannot manage users with higher-level roles (e.g., a Tenant Administrator or Global Administrator). Account Managers cannot perform endpoint management, and therefore cannot belong to any user group.
- **Endpoint Group Creator:** This role is specific to a particular tenant. It can perform endpoint management, as well as create new endpoint groups and manage Intel AMT Profiles. An Endpoint Group Creator can be a member of multiple user groups and can manage all groups to which they belong. Endpoint Group Creators cannot perform user management. However, they can see the list of all user groups and the list of all Endpoint Group Creators and Endpoint Group Users in that tenant (i.e., user roles in that tenant that are equal or lower in the user role hierarchy; they cannot see Account Managers, Tenant Administrators, or Global Administrators).
- **Endpoint Group User:** This role is specific to a particular tenant, and can perform endpoint management only. Endpoint Group Users can be members of multiple user groups, but they cannot perform user management, and can only view their own user information.

### 1.2.3 Endpoint Groups

An endpoint group is a collection of endpoints that share a common configuration and permissions. An endpoint can only join 1 endpoint group, but can change to different endpoint group. When you create an endpoint group, you must specify the following common setup:

1. The policy set: This policy set controls what actions can be executed on the endpoints in this endpoint group. Section 3.4.1 provides more details.
2. Intel® AMT auto-setup: Intel® EMA will try to set up all endpoints that join this endpoint group with this common Intel AMT configuration.

When you need to configure/set up an endpoint to connect to the Intel® EMA server, you need to download and run the Intel® EMA Agent installer with the policy file of the target endpoint group. Then the endpoint will connect to the Intel® EMA server and join the endpoint group specified in this policy file.

### 1.2.4 User Groups

A User Group is comprised of a list of users (Endpoint Group Creators or Endpoint Group Users) and the Endpoint Groups those users can interact with. A user can be a member of multiple user groups (User B in the figure below). An Endpoint Group and a user must be associated with the same User Group in order for the user to perform actions on that Endpoint Group (User B can perform actions on Endpoint Group 2

because they are both in User Group 1). An exception to this is Tenant Administrator users, who are not members of any groups but can still perform actions on any Endpoint Group.

The access permissions granted to the User Group determine the actions that can be taken by member users.

User Groups are assigned specific access permissions, such as Desktop, Terminal, Power Operations, USB Redirection, and more. You can select all permissions, or individually select specific permissions for this group.

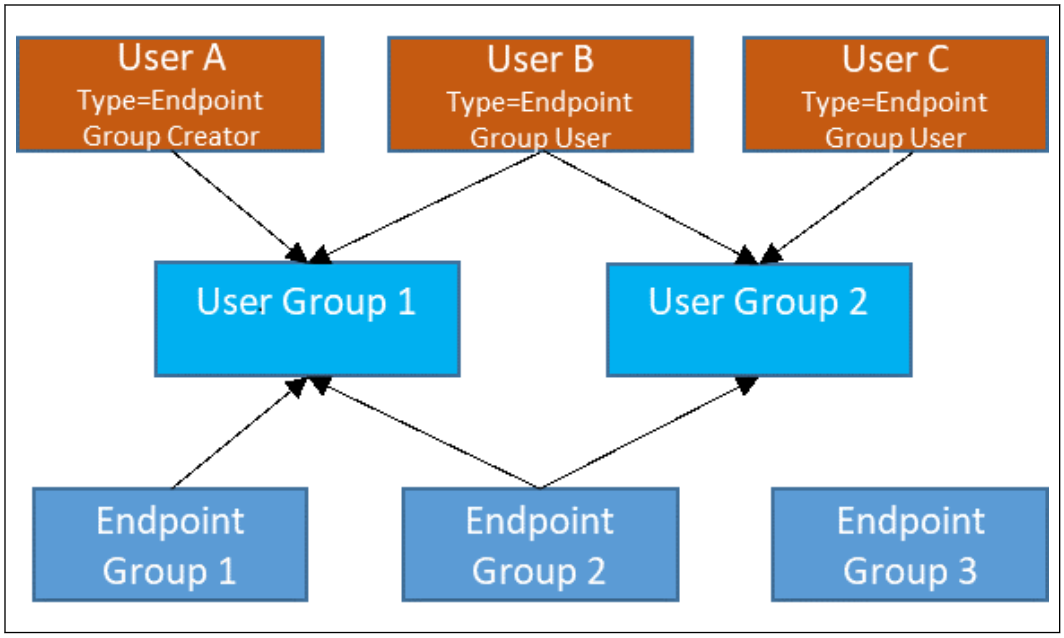
- User Groups are assigned specific access permissions, such as Desktop, Terminal, Power Operations, USB Redirection, and more. You can select all permissions, or individually select specific permissions for this group.

**NOTE**

A user who belongs to multiple user groups will have all permissions for all user groups to which they belong. For example, if User Group 1 has only Terminal permission, but User Group 2 has Power Operations permission, then User B will have both Terminal and Power Operations permissions for Endpoint Group 2 (which belongs to both user groups). However, User B will only have Terminal permission for Endpoint Group 1, which only belongs to User Group 1.

- Endpoint Group Creators and Endpoint Group Users within a Tenant can be associated with zero or more User Groups.
- Endpoint Groups within a Tenant can be associated with zero or more User Groups.

**Figure 2. Relationship between Users, User Groups, and Endpoint Groups**



## 1.2.5 Intel® EMA Agent

The Intel® EMA Agent is software that is installed on a client endpoint. The Intel® EMA Agent helps the client endpoint connect to the Intel® EMA server, enabling the Intel® EMA server to manage the endpoint. The agent actually consists of two files, EmaAgent.exe and EmaAgent.msh, which must both be present on the managed endpoint for the agent to work (Refer Deploying the Agent to Your Endpoints on page 49).

The agent also has a command line interface that can be used to display basic information about the agent's connection to the server. This can be helpful when troubleshooting the connection during agent deployment to the endpoints. (Refer s for more information.

### 1.2.5.1 Agent Prerequisites

**NOTE**

The Intel® EMA Agent is not designed to run in a VM on the target endpoint, even on the Base Hypervisor. The LAN/WLAN cannot interpret multiple IP addresses correctly. No Hypervisor has been written to accommodate the address translation required to use Intel AMT. This affects the agent's ability to connect to Intel AMT and perform Out of Band (OOB) actions on the endpoint. It is possible that in-band actions may work in this scenario, but that is not certain.

This is a list of the prerequisites needed to set up the Intel® EMA Agent:

- **Operating System:** Intel® EMA Agent is officially supported on Microsoft Windows 10 and Windows 11, 64bit operating systems. The 32bit agent has been deprecated and will no longer be released. Systems running the 32bit agent should be updated (a manual update procedure).
- **Firewall:** When Intel® EMA Agent is installed, it will set up the following Windows Firewall in-bound rules for the installed agent binary process. If you are using a different firewall, make sure that the following in-bound rules are set for the installed agent binary process:
  - Peer-to-peer traffic: UDP with local port at 16990, any IP for local and remote addresses, and edge traversal blocked.
  - Peer-to-peer traffic: TCP with local port at 16990, any IP for local and remote addresses, and edge traversal blocked.
  - Local loopback management traffic: TCP with local port at 16991, 127.0.0.1 for local and remote addresses, and edge traversal blocked.
- Intel® Active Management Technology (Intel® AMT): Intel® EMA only supports Intel® AMT 11.8.79 or later Only required for Out-of-band endpoint management. Refer In-band vs. Out-of-band on page 15

  The following table lists the minimum Intel AMT versions required on endpoints to use USBR over CIRA.

| Intel AMT Version | Build Number |
|---|---|
| Intel AMT 11 | 11.8.79 or later |
| Intel AMT 12 | 12.0.70.1607 or later |

*continued...*

| Intel AMT Version | Build Number |
|---|---|
| Intel AMT 14 1 | 4.0.45.1341 or later |
| Intel AMT 15 | all |
| Intel AMT 16 | all |

For more information about USBR, refer USB Redirection on page 18.

#### 1.2.5.2 Agent Windows Registry Information

Registry keys created by the Agent's installation depend on the architecture of the Microsoft Windows OS and the Intel® EMA Agent (console and service). These are the registry paths for Intel® EMA Agent by architecture:

- Win64 Service:

  HKEY_LOCAL_MACHINE -> "Software\Intel\EmaAgent"
- Win64 Console:

  HKEY_CURRENT_USER -> "Software\Intel\EmaAgent"

The following registry keys should exist at this reg key root when the Intel® EMA Agent is installed/running:

- **MeshId** - REG_SZ that contains the Endpoint Group ID from the MSH file; if no MSH file is present, then this value will be empty.
- **MeshName** - REG_SZ that contains the Endpoint Group Name from the MSH file; if no MSH file is present, then this value will be empty.
- **NodeId** - REG_SZ that contains the Endpoint ID.

  **NOTE**

  Endpoint ID is tied to the Agent root certificate. Different root certificates are used for service/console.

- **Version** - REG_DWORD that contains the version number of the running EmaAgent.
- **EnhancedLoggingLevel** - REG_DWORD that contains the logging level. By default this is set to 3, which disables enhanced debug logging. To enable enhanced debug logging, edit the registry and set EnhancedLoggingLevel to 4.

### 1.2.6 In-band vs. Out-of-band

The Intel® EMA Agent runs in the operating system on a managed endpoint. We call this connection an "in-band" connection. All the features that rely on this connection are called in-band features. All the features that rely on Intel® AMT are called out-of-band features.

**NOTE**

In-band features require a working operating system to be running on the managed endpoint. To interact with an endpoint whose operating system is not working or not present, you must use an out-of-band connection via Intel AMT.

Once Intel AMT is set up on an endpoint, Intel® EMA can talk to Intel AMT via one of the following approaches:

- TLS Relay: In this approach, other Intel® EMA Agents relay the Intel AMT command to the target Intel AMT on the target endpoint. To be a relay, the agents need to be in the same subnet and registered to the same endpoint group. When an endpoint restarts, its agent broadcasts to the other Intel® EMA agents in the group/subnet, establishing contact with its "neighbors" for TLS relay. When the Intel® EMA Agent talks to the target Intel AMT, it will use the Intel AMT TLS port. This is why it is called TLS Relay.
- Intel® AMT CIRA (Client Initiated Remote Access): Intel AMT CIRA can be used with either DHCP or static IP addresses. In this approach, the endpoint system's Intel AMT connects to the Intel® EMA Server via a TCP TLS connection at Swarm Server port[1] (note that the in-band Intel® EMA Agent also connects to the Intel® EMA server via TCP TLS at Swarm Server port[1]). Intel AMT CIRA creates its own encrypted tunnel, so that additional TLS is not needed. Intel AMT will try to connect several times when CIRA is enabled or when the endpoint system is rebooted. However, if all attempts fail, Intel AMT will not continue trying to connect until the next time the endpoint system is rebooted. Once connected, though. CIRA will maintain communications between the Intel® EMA server and the endpoint so that the endpoint can always reach the server.

  If the Intel AMT profile is set to use DHCP, then Intel AMT CIRA makes use of the Intel AMT feature "environment detection." When the endpoint system's network domain matches the configured CIRA domain, Intel AMT will not start the CIRA connection. In this case, the Intel® EMA server uses the communication approach similar to TLS Relay. When using static IP addresses, the "environment detection" feature is ignored, and CIRA will always connect.

  When using DHCP, you can force Intel AMT to always open a CIRA tunnel by selecting "Always Use Intel AMT CIRA" or by entering a fake domain suffix in the CIRA intranet suffix field under General settings when creating your Intel AMT profile. This fake domain suffix should be complex enough to prevent anyone from guessing it and thus using it to prevent a CIRA connection and open local management ports. Refer to the General Settings on page 39.

**NOTE**

[1] Default Swarm server ports are 8080 and 8081. Legacy port (8080) uses 2048-bit key sizes and will be used for systems provisioned before updating to Intel® EMA 1.15.0, systems that do not support larger keys, or agents that are members of endpoint groups created before the update. New port (8081) uses 3072-bit key sizes and will be used by endpoints provisioned after updating to Intel® EMA 1.15.0 that support 3072-bit keys, or agents that are members of endpoint groups created after the update.

### 1.2.7 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 (Enable Intel AMT Auto-Setup on page 46), or manually perform an on-demand setup of Intel AMT (Intel® AMT On-demand Setup on page 59).

**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. Intel AMT Profiles, and uploading PKI certificates for them, are discussed in Create Your Intel AMT Profiles on page 38.

**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. Refer Setting or Verifying the Correct PKI DNS Suffix in Intel® MEBX on page 45 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.

**NOTE**

For unprovision (deactivation) of Intel AMT, if the unprovision fails, Intel® EMA will automatically retry it every three minutes until it is successful or until one hour passes without success. In all cases (Round 1, Round 2, or unprovision), if Intel® EMA is disconnected from the endpoint, it will retry whichever process it was attempting upon reconnecting to the endpoint.

#### 1.2.7.1 Unprovisioning

If the endpoint is in Intel® AMT Client Control Mode, Intel® EMA tries to use Intel® EMA Agent to issue a CFG_Unprovision command via Intel® MEI driver, to reset Intel AMT to default factory settings.

If the above fails or the endpoint is in Intel AMT Admin Control Mode, Intel® EMA sends to WSMAN request AMT_SetupAndConfigurationService\Unprovision to reset Intel AMT to default factory settings.

Intel® EMA also tries to clear/remove the Active Directory objects created for 802.1X configuration, if this endpoint group is using an Intel AMT Profile with 802.1X setup.

**NOTES**

- An instance of Intel® EMA can only unprovision endpoints which it has provisioned. Endpoints provisioned by one Intel® EMA instance cannot be unprovisioned by another instance. Note that in a distributed server environment, all the servers in that distributed server environment are considered the same Intel® EMA instance.
- 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.

### 1.2.8 USB Redirection

The USB Redirection (USBR) and One Click Recovery (OCR) features of Intel® EMA allows you to mount a remote disk image (.iso or .img) to a managed endpoint via Intel AMT. You can use this feature to mount a bootable image file and reboot a managed endpoint to a mounted image file, or browse the mounted image content from the console of the managed endpoint via KVM (image must contain USB keyboard and mouse drivers for KVM interaction). Once you have mounted an image file, you can reboot the endpoint to the mounted image. Refer Mount an Image on page 70 for details on how to mount an image to a managed endpoint. Refer Boot to This Image on page 71 for details on rebooting to a mounted image.

**NOTES**

- CIRA based provisioning is highly recommended when using USBR. USBR is sensitive to latency and Intel® EMA has optimized USBR for CIRA provisioned endpoints. If you are using TLS with relay, you will need to adjust the "USBR Redirection Throttling Rate" under the Manageability Server section in Server Settings as a Global Admin. This setting is dependent upon your unique network environment. We recommend starting at a setting of 10 milliseconds and increasing it in increments of 10 until you find a rate that works well in your network environment. It is unlikely you would need to go above of 50 milliseconds. Note that increasing this setting will decrease the USBR boot performance, especially for CIRA endpoints, and should only be used for TLS with relay only instances. Refer In-band vs. Out-of-band on page 15 for information about CIRA. Refer Manageability Server on page 83 for information on setting Manageability Server settings.
- It is strongly recommended that you do not upload confidential data.

The Storage page, accessible from the navigation pane at left in the Intel® EMA UI, lets you upload and store image files (.iso or .img) for later use in mounting to endpoints. Refer Managing Disk Images on page 74 for details.

The following table lists the minimum Intel AMT versions required on endpoints to use USBR over CIRA.

| Intel AMT Version | Build Number |
|---|---|
| Intel AMT 11 | 8.79 or later |
| Intel AMT 12 | 0.70.1607 or later |
| Intel AMT 14 | 0.45.1341 or later |
| Intel AMT 15 | all |
| Intel AMT 16 | all |

## 1.2.9 Remote Secure Erase

Remote Secure Erase (RSE) is an Intel AMT feature which allows IT administrators to remotely erase the hard disk of a client device. This feature is available in the Intel® EMA user interface on the Hardware Manageability tab (refer Hardware Manageability Tab on page 62), as well as in the Intel® EMA API. See the Intel® EMA API Guide for details on specific API calls for using Intel® EMA's RSE implementation.

The RSE feature can be useful when an employee leaves an organization, in which case their IT department can remotely erase the entire drive (bootable partition) and then use Intel® EMA's KVM and USBR features to remotely reinstall operating systems and applications to the device so it can be issued to another employee.

**NOTE**

In order for Intel® EMA to perform this feature on a device (either via the user interface or the API), the target device (12th Gen Intel® Core™ platform or later) must be a managed endpoint in Intel® EMA and its Intel AMT must be provisioned by Intel® EMA. Further, the target device must have a BIOS and hard disk drive that supports this feature.

For more information on Intel AMT's Remote Secure Erase feature, and its requirements, see the Intel AMT Developers Guide at the following link:

https://software.intel.com/content/www/us/en/develop/documentation/amt-developer-guide/top/remote-secure-erase/remote-secure-erase-implementation.html

**NOTE**

When using the Intel® EMA API, if the attempted erase operation fails, the Intel AMT boot options are not cleared. This boot options data must be cleared before retrying the erase operation. Intel® EMA provides an API, **POST /api/latest/endpointOOBOperations/Single/SecureErase/{endpointId}/clear**, which will clear the Intel AMT boot options on the specified device so that the erase operation can be retried. See the Intel® EMA API Guide for details on this specific API call.

### 1.2.10 Intel® Remote Platform Erase Overview

Intel® Remote Platform Erase (Intel® RPE) allows you to remotely erase all platform information, including (optionally) the platform's Intel AMT information. This allows you to reuse the platform without manually erasing the SSD.

**NOTE**

In order for Intel® EMA to perform this feature on a device (either via the user interface or the API), the target device (12th Gen Intel® Core™ platform or later) must be a managed endpoint in Intel® EMA and its Intel AMT must be provisioned by Intel® EMA. Further, the target device must have a BIOS and hard disk drive that supports this feature.

With Intel RPE, you can protect company assets and personal information by clearing all user and company data from the device before disposing of or reselling the device.

For information on how to use this Intel AMT feature from within the Intel® EMA user interface, refer Boot to Recovery Image on page 71.

For more information on Intel RPE, see the Intel AMT Developers Guide at the following link:

https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/WordDocuments/Secure_Remote_Platform_Erase.htm

### 1.2.11 One Click Recovery

One Click Recovery (OCR) allows you to initiate a recovery process on a specified endpoint.This feature allows you to return the endpoint's OS to a last known good state, as well as recover from a bad state, bare-metal situation, or connectivity issues. Intel AMT Out-of-Band (OOB) capability is required for this feature.

**NOTE**

In order for Intel® EMA to perform this feature on a device (either via the user interface or the API), the target device (12th Gen Intel® Core™ platform or later) must be a managed endpoint in Intel® EMA and its Intel AMT must be provisioned by Intel® EMA. Further, the target device must have a BIOS and hard disk drive that supports this feature.

Intel® EMA implements this feature by installing and deploying a Recovery Server as one of its component servers. For information, refer Recovery Server Settings on page 90.

The Intel® EMA implementation of One Click Recovery allows you to use preconfigured recovery images from the endpoint itself as well as images you have uploaded to the Intel® EMA server (refer Boot to Recovery Image).

If you plan to select and use recovery images that use HTTPS, you must enable HTTPS boot in the endpoint's BIOS as follows:

1. **Enable secure boot in BIOS:** Boot Maintenance Manager Menu > Secure Boot Config Menu > Attempt Secure Boot = Checked
2. **Enable HTTPS Boot in BIOS:** BIOS Menu path–Intel Advanced Menu > PCH-IO Configuration > EFI Network <Onboard NIC>
3. **Change Boot order and make HTTPv4 the priority**:
   a. Boot to Bios > Boot Maintenance Manager Menu
   b. Boot Options Menu > Change Boot Order
   c. Save and Restart.

For further information about One Click Recovery, see the Intel AMT online documentation at the link below:

https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/WordDocuments/oneclickrecovery.htm

### 1.2.12 Microsoft Entra ID Authentication

- During first time login, user can be come across the below possible scenarios:
- — If the user was added manually in the Intel® EMA and not assigned to any ID group, then the user will be able to login as long user exist in Microsoft Entra ID.
  — If the user does not exist in Intel®EMA, then the user should be a member of Microsoft Entra ID security group and that group must be added to Intel®EMA prior to login. If this is the case, then after successful login; Intel®EMA will create the user and will associate Microsoft Entra ID with that user. User role will be determined:
  — • If the user is a member of more than one Microsoft Entra ID security groups, then the user will be assigned with the highest priority role.
    • If the user is a member of only one Microsoft Entra ID security group then the user will be assigned with same role as security group.
- During user login, Intel® EMA will upgrade or downgrade the role of the user based on role of Microsoft Entra ID group associated with user.

### 1.2.13 Intel LMS Features and Installation

Intel Local Manageability Service (Intel LMS) is a service that can enhance your Intel® EMA usage experience by enabling the use cases below. Intel LMS is not a part of Intel® EMA, and is not required for Intel® EMA to function as designed, since Intel® EMA does include a "micro LMS" built in. However, Intel LMS does facilitate the following use cases on managed endpoints, which are not supported unless the full Intel LMS service is installed on the endpoints.

**NOTE**

If Intel LMS is present on a managed endpoint, Intel® EMA will automatically use it instead of the built-in micro-LMS. If Intel LMS is not present on your endpoints, refer to the section below.

#### 1.2.13.1 Features and Use Cases

- Intel Management and Security Status (Intel IMSS) - required for privacy
- Time Sync
- WiFi Profile Sync
- Static IP Sync
- WMI Provider
- Logging events in system event log
- Graceful reset (though the Intel® EMA agent handles this within Intel® EMA)

For further information about Intel LMS see the Intel AMT Reference Guide at the link below:

https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm?turl=WordDocuments%2Flocalmanageabilityservice.htm

#### 1.2.13.2 Obtaining and Installing Intel LMS

Many PC OEMs distribute Intel LMS on their PC platforms. If you have endpoints that do not have Intel LMS installed, you can do the following to obtain and install Intel LMS on your managed endpoints:

1. Go to https://www.intel.com/content/www/us/en/download/682431/intel-management-engine-drivers-for-windows-7-windows-8-1-and-windows-10.html.
2. On the managed endpoint, download the latest Intel Management Engine (Intel ME) driver package zip file (**ME_SW_<version>.zip**).
3. When the download completes, unzip the downloaded file on the managed endpoint.
4. Open the extracted folder (**ME_SW_<version>**), then open the **Drivers > LMS** folder.
5. Right click **LMS.inf** and choose **Install**.
6. Once the installation is complete, open Device Manager and ensure the device **Intel(R) Management and Security Application Local Management** is displayed.

### 1.2.14 Important File and Directory Locations

| | |
|---|---|
| <Installer Directory>/EMALog-Intel®EMAInstaller.txt | Installation log |
| C:\Program Files (x86)\Intel\Platform Manager \Platform Manager Server\settings.txt | Contains settings for the Platform Manager, including the port number and password. |
| C:\Program Files (x86)\Intel\Platform Manager \Runtime\MeshSettings\app.config and connections.config | Contains the database connection string (encrypted). |
| C:\Program Files (x86)\Intel\Platform Manager \EMALogs<br>• EMALog-XXX.txt<br>• TraceLog-XXX.txt | A log for each server component. These are the same log messages that you can see in the Platform Manager's Event log. |
| C:\Program Files\Intel\Ema Agent | Install location for 64 bit Intel® EMA Agent files. |
| C:\inetpub\wwwroot | IIS web site locations. |

# 2.0 Logging in to Intel® EMA

To log in to Intel® EMA, do the following:

1. Open a browser and navigate to the FQDN/Hostname specified during installation (if unsure, consult your Intel® EMA Global Administrator). In a distributed server installation, this will be the URL of the Ajax and Web server load balancer.
2. Login with Azure SSO Credentials or SAML Authentication credentials, if you installed Intel® EMA with Azure AD or SAML Authentication respectively, otherwise use Login with Intel® EMA Credentials. Otherwise proceed to step 4.

   **NOTE**

   If this is the initial login in Azure AD mode or SAML authentication immediately after installation, you must choose Login with Intel® EMA Credentials and enter credentials for the initial user you created during installation. and configure your webserver settings to do a proper setup.

3. For Azure SSO credentials, enter the appropriate Microsoft Azure single sign on credentials, or for SAML SSO credentials, enter the necessary SAML authentication credentials.
4. For Intel® EMA credentials, enter the user name (i.e., email address) and password for the Tenant Administrator user assigned to you by the Global Administrator. For other users, enter the username and password assigned to you by the Tenant Administrator or Account Manager.

   **NOTES**

   - The Intel® EMA website user interface (UI) uses cookies. If you disable cookies in your browser, the Intel® EMA website UI will not work.
   - Depending on how Intel® EMA was installed, the Overview page may be automatically displayed, or you may be asked for Intel® EMA credentials first.
   - If you are logged into Intel® EMA and open a new tab in your browser, you will be taken to the login page. You can change this by changing from sessionStorage to localStorage in Intel® EMA's web server settings on the Server Settings page (refer to the *Appendix - Modifying Component Server Settings)*, but be aware that some browsers do not share session cookies across tabs.
   - Logging in as a different user on a new tab (when already logged into Intel® EMA in another tab) is not supported. You can complete the login on the new tab, but errors will be displayed on the original login tab.
   - If you enter an incorrect password too many times, your account will be locked for 24 hours. If this happens, consult your Global Administrator.

## 2.1 Overview Page

Once you log in to Intel® EMA, an Overview page is displayed. The contents of this page varies depending on which user role you are logged in as. The figure below shows the Tenant Administrator's Overview page.

**NOTE**

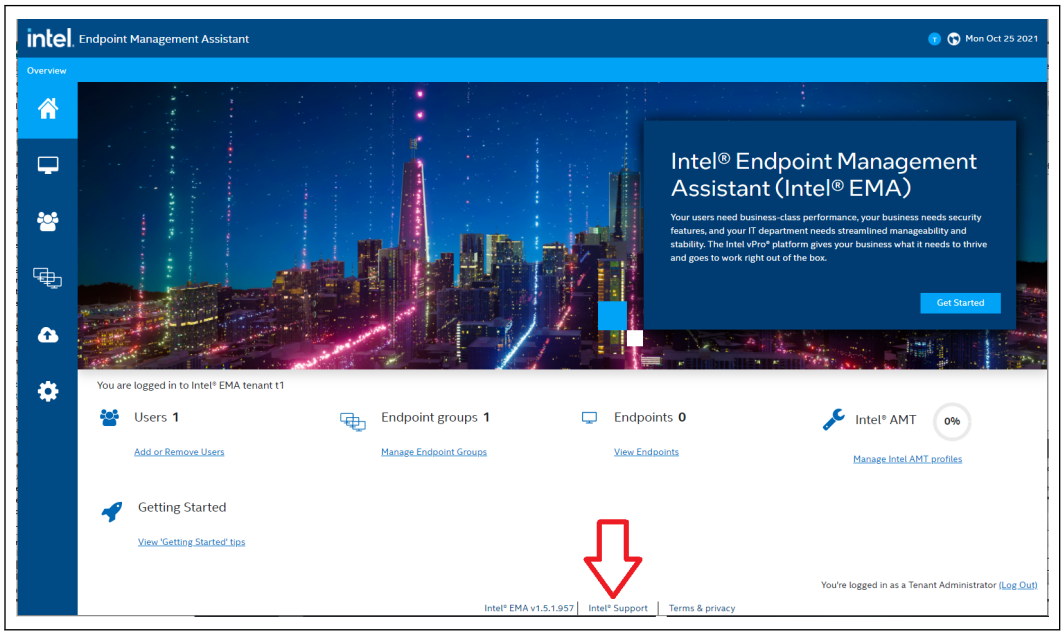
The first time you log in, a Getting Started link is displayed. This page is displayed until you create your first Endpoint Group. Tasks in the Getting Started page are described in more detail, refer

Setting Up Your Tenant(s)

The quick links at the bottom provide easy access to most Tenant Administrator tasks, which are covered in the subsequent sections of this guide.

For assistance, click the **Intel Support** link at the bottom of the page.

**Figure 3. Tenant Administrator Overview**




### 2.1.1 Adding or Removing Server Name from Footer

By default, the footer of the Intel® EMA web UI page does not display the name of the Intel® EMA server. However, you can add it to the footer if desired using the following instructions.

1. On the Intel® EMA server machine, open IIS.
2. In the left-hand navigation pane, select **Default Web Site**, then select **Configuration Editor**.
3. Open **appSettings**.

4. Add an item to the list of items with "name2" for the **key** column and "(<server_name>)" for the **value** column, where <server_name> is the name of the Intel® EMA server.

   **NOTE**

   Value column is a simple string, so whatever you type within the required parentheses is what will be displayed in the footer.

5. Save the configuration and exit ISS. The next time you launch Intel® EMA, you should see the server name in the footer at the bottom.

## 2.2 Setting up Two Factor Authentication

To improve the Intel® EMA security, we have added the option for Two factor Authentication (2FA) using Time-based One-Time Password (TOTP).

By default, 2FA is enabled under Normal authentication (Username and Password). However, Global Administrator can also enable this under **Server Settings** option. You can chose the desired encryption algorithm depending on the values supported by the authenticator tool of your preference.

**NOTE**

The National Institute of Standards and Technology (NIST) deprecated the use of SHA1 and recommends moving away from SHA1 as soon as possible. Additionally, SHA256 is now considered deprecated by Intel and Intel recommends against its use as well. We advise you to use the highest level of encryption possible and to work with your authenticator application providers to leverage more robust algorithms. Be aware that SHA1 and SHA256 support will be eliminated in future Intel® EMA releases.

**NOTE**

When selecting the encryption algorithm, Read the documentation of authenticator app you are using to make sure it supports the hashing algorithm set in Intel® EMA security settings.

### ENABLE 2FA WITH TOTP

- Select the algorithm to be used to define the secret size.

  **NOTE**

  Option to enroll in the 2FA method is only available for users in all roles with 'normal' accounts. This option will not be available for Client Credentials.

- Users can now individually enable 2FA for their account from their own **User Settings** menu at the top right of the page through the **Manage 2FA** option.
- Using the authenticator app of your preference, follow the instructions by either scanning the QR code presented in the first screen or copying the link in the **Additional Enrollment** options.

**NOTE**

Read the documentation of authenticator app you are using to make sure it supports the hashing algorithm set in Intel® EMA security settings by your Administrator.

- The last screen will show the six recovery codes which should be kept in a secure place to recover access to your account in case of access issues to the authenticator app. You can copy-paste these codes in a secure place.
- Once the user clicks **Next** on this screen, a final confirmation screen will be displayed. At this point, the user account is now enrolled to use **2FA with TOTP**.
- Click **Finish** to complete the operation and the user will be logged out from the current session to log back in again now using a 2FA code.

### Logging in using 2FA with TOTP

1. Users enrolled in the 2FA option will be required to enter the 2FA code provided by their authenticator app upon login.
2. After entering the username and password, a new screen is prompted asking for the 6 digit 2FA code.

**NOTE**

Failure to enter the correct code too many times will cause the user to be locked out of Intel® EMA for 24 hours. This follows the same behavior when the regular password is entered incorrectly too many times.

- Number of max failed login attempts can be configured from the **Server Settings** section by the Global Administrator

### Unenroll From 2FA

Only higher privilege users or each user individually can unenroll from 2FA by performing one of the two options mentioned below, depending on their access level:

- **Unenrolling other users:**

  Higher privilege users in roles: **Tenant Admin**, **Account Manager** or **EGC** have the option to unenroll other users accounts from 2FA.

  1. From the **User Administration** section, go to **2FA** column indicating users who have enrolled in 2FA. It will also indicate those who are not eligible for 2FA.
  2. Select the option **Unenroll 2FA** for the desired user.
  3. A confirmation prompt will be displayed.
  4. Check the confirmation message to make **Unenroll User From 2FA** button available.
  5. Click **Continue** on the next screen to finish the process. Any active token for that user will be immediately disabled.
- **Users Unenrolling Themselves:**

  1. For all users, they can disable their 2FA subscription through the **User Settings** menu at the top right of the page through the **Manage 2FA** option.

2. For users with access to account management, they can use the **Unenroll 2FA** option from the **User Administration** section.
   a. Select the option **Unenroll 2FA** for the desired user. A confirmation prompt will be displayed.
   b. Check the confirmation message to make **Unenroll User From 2FA** button available.
   c. Click **Continue** on the next screen to finish the process. Any active token for that user will be immediately disabled.
3. A confirmation screen will request for your 6 digit 2FA code to enable the **Continue** button.
4. Click **Finish**. This will immediately disable your active tokens and you will be logged out of Intel® EMA.

# 3.0 Setting Up Your Tenant(s)

This section describes how to set up and configure a particular Tenant on the Intel® EMA server. Unless otherwise noted, the tasks in this section are performed by the Tenant Administrator user. Actions which can be performed by other users are noted at the beginning of that action's subsection.

**IMPORTANT**

You must be logged in to the Intel® EMA server as a user with Tenant Administrator privileges to perform the steps in this section. As described in Section 3 of the Intel® EMA Server Installation and Maintenance Guide or the Intel® EMA Distributed Server Installation and Maintenance Guide, the Global Administrator should have already created at least one Tenant and Tenant Administrator user as part of the Getting Started steps following the Intel® EMA installation. Refer to these installation guides if necessary.

**NOTE**

Not all of the tasks in this section may be required, depending on your organization. Furthermore, many of the tasks, such as adding new users and creating new endpoint groups, may be performed regularly over time as your organization grows and changes.

Below is the basic process for setting up your Tenant. These steps are explained in detail in the subsequent subsections.

1. **Create your Endpoint Groups** - Endpoint Groups are logical groupings of endpoints, based on your organization. For example, you could have an Endpoint Group for your Accounting department, and another for Engineering. This allows you to have different IT policies for different groups. We recommend that you fully configure an Endpoint Group by completing the remaining steps in this process, then return to this step as needed to create and configure additional endpoint groups. **Roles**: Tenant Administrator, Endpoint Group Creator.
2. **Create the Intel® EMA Agent files for each Endpoint Group** - Regardless of whether you plan to use OOB features or not, you must install and configure the Intel® EMA Agent on your endpoints in order for Intel® EMA to manage them. This step creates a pair of Agent files based on your Endpoint Group configuration (policies, Intel AMT profile, etc.). **Roles:** Tenant Administrator, users with appropriate access permissions based on group association.
3. **Create your network profiles** - If you plan to use WiFi or 802.1X in your production environment, you can configure profiles for these networking technologies which can be easily selected when creating Intel® AMT profiles. You can also create these network profiles as part of the Intel AMT profile creation flow, but if you plan to re-use network profiles in multiple Intel AMT profiles, it may be easier to create the network profiles in advance. **Roles**: Tenant Administrator. If you will not be using WiFi or 802.1X in your environment, you can skip this step (Section 3.1).

4. **Create your Intel® AMT profiles** - If you plan to use Out-of-Band (OOB) features to manage your endpoints (i.e., endpoint management features that work when the endpoint's operating system is unavailable), you must configure Intel AMT on your endpoints. You can manually configure Intel AMT on each and every endpoint, or you can have Intel® EMA set up Intel AMT on all your endpoints automatically. In order for Intel® EMA to automatically set up Intel AMT, you must configure at least one Intel AMT profile for Intel® EMA to use. **Roles:** Tenant Administrator, Endpoint Group Creator.

   If you do not want to use Intel AMT auto-setup, you do not need to configure Intel AMT profiles and can skip this step (Section 3.2).
5. **Upload your Intel® AMT PKI certificates** - Intel AMT PKI certificates are used for PKI provisioning, and are required if you plan to enable Intel AMT auto-setup in Admin Control Mode. If you do not have an Intel AMT PKI certificate, or want to enable Intel AMT auto-setup in Client Control Mode, skip this step (Section 3.3). **Roles**: Tenant Administrator.
6. **Enable Intel® AMT auto-setup** - As mentioned above, Intel AMT auto-setup allows Intel® EMA to automatically set up Intel AMT on your endpoints. Intel AMT must be set up on your endpoints if you plan to use Intel® EMA's OOB endpoint management features. You must have an Intel AMT PKI certificate and an Intel AMT profile to enable Intel AMT auto-setup in ACM mode. **Roles**: Tenant Administrator and users with appropriate access permissions. If you do not want to enable Intel AMT auto-setup on your endpoints, you can skip this step (Section 3.5).
7. **Deploy the Intel® EMA Agent files to the managed endpoints** - Once you have created your Intel® EMA Agent files, you need to deploy them to your endpoint systems. This section provides instructions for manually installing the agent files directly on a given endpoint system, using either the command line or a GUI installer. The command line procedure can be leveraged to create automated deployment packages using a mass deployment tool. **Roles**: Any user with admin rights on the managed endpoint system.
8. **Create additional users and user groups as needed** - Depending on the size and complexity of your organization, you may decide you need additional users to help manage your endpoints ( refer User Roles on page 11 for information on user roles). These users can be grouped into User Groups as needed. **Roles**: Tenant Administrator, Account Manager.

## 3.1 Create Your Endpoint Groups

Endpoint Groups are logical groupings of endpoints, based on your organization. For example, you could have an Endpoint Group for your Accounting department, and another for Engineering. This allows you to have different IT policies for different groups.

Each endpoint group has an associated policy set. The policies in a set include the following:

| | |
|---|---|
| **Power Operations** | • **Wake-up**: If this policy is selected, remote wake-up/boot-up of the endpoint is enabled.<br>• **Sleep**: If this policy is selected, remote activation of sleep and hibernate modes on the endpoint is enabled. |

***continued...***

| | |
|---|---|
| | • **Turn off or restart**: If this policy is selected, remote power-off and restart of the endpoint are enabled. |
| **Messaging and Alerts** | • **TCP traffic relay**: This policy forms the base of all the following policies. If this policy is not chosen, the endpoint can still connect to an Intel® EMA server. However, Intel® EMA cannot perform any operation on the endpoint, including Intel® AMT setup.<br>• **Alert messages**: If this policy is selected, display of alert messages on the endpoint is enabled.<br>• **Console prompts**: If this policy is selected, running scheduled remote execution on endpoints is enabled. This policy should be used to control remote terminal access. For out-of-band terminal access, the Intel AMT profile used during Intel AMT setup needs to enable this policy also.<br>• **Peer-to-peer communication**: This policy applies to the communication among endpoints (Intel® EMA Agents) that are in the same network. If this policy is not selected, agents will not look for other agents within their network, and will not accept communication from other agents. Therefore, the features that require Intel® EMA Agent relay (such as Intel AMT setup under "TLS with relay") will not work. |
| **Remote Control** | • **Remote KVM:** If this policy is selected, remote KVM is enabled. For out-of-band KVM, the Intel AMT profile used during Intel® AMT setup needs to enable this policy also.<br>• **Remote file access:** If this policy is selected, remote in-band file access (by file browser, scheduled file delivery, or file search) to the endpoint is enabled.<br>• **Remote management (WMI):** If this policy is selected, remote WMI queries and remote process operations (via WMI) on the endpoint are enabled. This policy also controls whether Intel® EMA can remotely set the endpoint to BIOS or not.<br>• **User consent for in-band KVM:** If enabled, the following logic is applied: If the target endpoint is not in user session (locked, logged out, etc.), then the KVM will be rejected upon the timeout. Else if the target endpoint is in user session, then the user will get a pop-up window to accept or reject. If the user agree, the in-band KVM goes through and a system tray icon on the target endpoint will show to indicate that it is in KVM session. Else if disabled, user consent is not needed. |

Regarding the out-of-band features (features provide by Intel AMT):

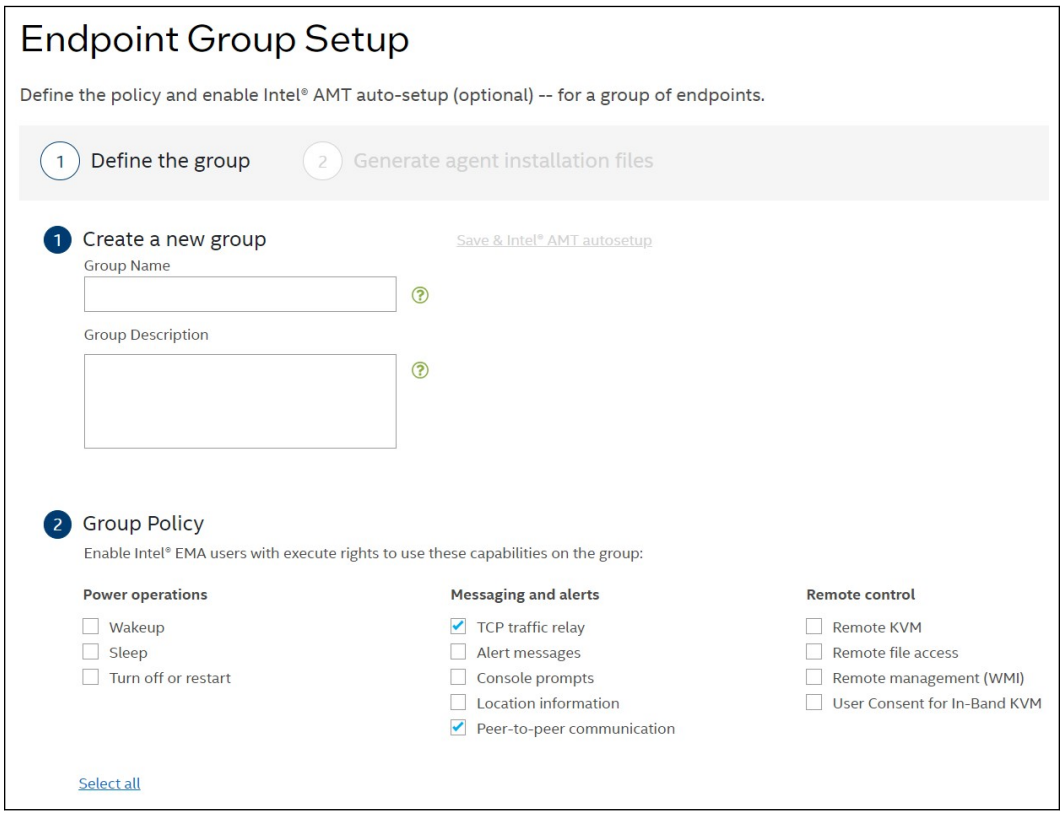
- Out-of-band terminal and out-of-band KVM are controlled by the Command policy and the KVM policy. If one of these policies is allowed, then both features are allowed.
- The following WSMAN power action is checked against the endpoint group policy specified: CIM_PowerManagementService \ RequestPowerStateChange.

### 3.1.1 Creating New Endpoint Groups

**Roles**: Tenant Administrator, Endpoint Group Creator

1. Select **Endpoint Groups** from the navigation bar at left, then select **New Endpoint Group**.
2. Fill out the fields and select the **Group Policy** capabilities that should be available for endpoints in the group.
3. If you plan to use WiFi or 802.1x profiles in your Intel AMT profiles, click **Generate agent installation files** and proceed to the Create Agent Files for Deployment to Managed Endpoints on page 33. You can enable Intel AMT autosetup after creating network profiles and Intel AMT profiles. If you want to go straight to setting up Intel AMT autosetup on the endpoints in this group, click **Save & Intel® AMT autosetup** and proceed to Create Your Intel AMT Profiles on page 38.

**Figure 4. Endpoint Group Setup page**




### 3.1.1.1 Automatic Endpoint User Group Creation (tag to admin usage only)

**Roles**: Endpoint Group Creator ONLY

When an Endpoint Group Creator user creates a new endpoint group, Intel® EMA automatically creates a user group with appropriate access permissions and includes the current user in the group. It also automatically associates this user group to the new endpoint group. This internally auto-created user group is named using the format [created endpoint group name]_EndpointGroupCreators. Thus, the access control to an endpoint group is still maintained by the user groups.

**NOTE**

Tenant Administrators who create a new endpoint group will not see this auto-created user group, because the Tenant Administrator does not belong to any particular user group.

## 3.1.2 Viewing and Deleting an Endpoint Group

**Roles**: Tenant Administrator (delete, view), Endpoint Group Creator (delete, view), Endpoint Group User (view)

An Endpoint Group Creator can only delete Endpoint Groups that belong to the same User Group (with Execute right) as the Endpoint Group Creator. An Endpoint Group Creator can only view Endpoint Groups that belong to the same User Group (with View right) as the Endpoint Group Creator.

An Endpoint Group User can only view Endpoint Groups which belong to the same User Groups as the Endpoint Group User.

Click the down-arrow next to the target endpoint group and select **View Configuration.**

To delete this endpoint group, click **Delete Group**.

**NOTE**

If you delete this endpoint group, then the endpoints in this group will be unable to connect to Intel® EMA server.

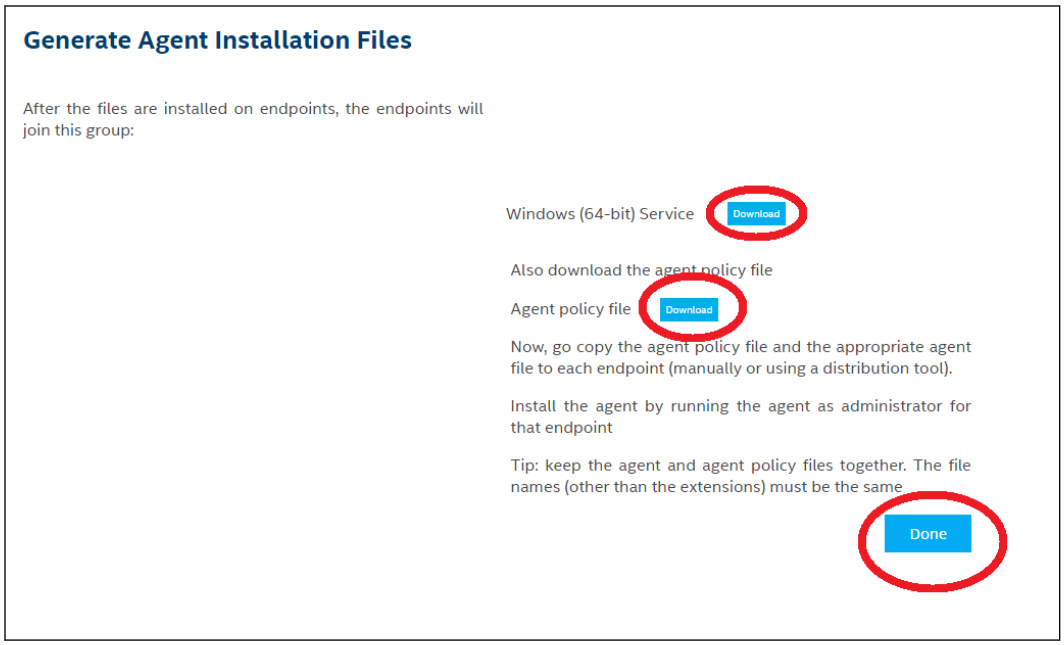
## 3.2 Create Agent Files for Deployment to Managed Endpoints

**Roles**: Tenant Administrator, Endpoint Group Creator†, Endpoint Group User†

†With access permissions for this group

1. If you are not continuing from the previous section, you can access this screen from the navigation bar at left, select **Endpoint Groups**, then click the down-arrow next to the target endpoint group and select **Create Agent Files**.
2. Click **Download** for the Windows 64-bit Service agent file.
3. Click **Download** for the Agent policy file, then click **Done**.

**Figure 5. Generate Agent Installation Files**



Both files are created in the Downloads folder on the system on which you are using the Intel® EMA web-based UI. Keep these files together and copy them to the endpoint systems you want to manage with Intel® EMA. That installation process is described in Deploying the Agent to Your Endpoints on page 49, but it is recommended that proceed to Create Your Network Profiles on page 34 and follow the subsections in order.

**NOTE**

- For information about associating your Endpoint Groups with User Groups to manage user access to them, refer Assigning Endpoint Groups to User Groups on page 57.

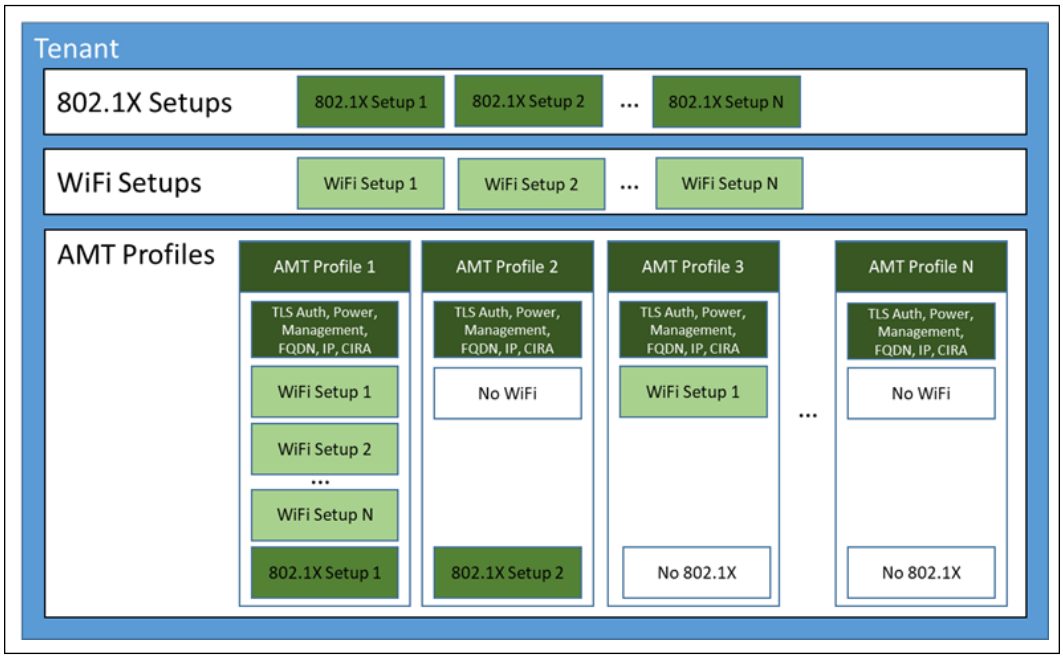
  For information about troubleshooting agent installation on endpoints, refer Verifying and Troubleshooting Agent Installation on page 51.

## 3.3 Create Your Network Profiles

**Roles**: Tenant Administrator

Although you can create network profiles when you create your Intel® AMT profiles, you may find it easier to create the network profiles in advance. That way you can simply select one of your existing network profiles when creating your Intel AMT profile. The figure below illustrates the relationship between network profiles, or "setups", and Intel AMT profiles.

**Figure 6. Network Profiles and Intel® AMT Profiles**




If you will not be using WiFi or 802.1X in your environment, you can skip this section.

## 3.3.1 Creating a New Wi-Fi Profile

### To Create a New Wi-Fi Profile:

Select **Endpoint Groups** from the navigation bar at left, then select **Intel® AMT Profiles > Manage WiFi Profiles** and click **New Profile**. You can also create a new WiFi profile as part of the Intel® AMT Profile creation workflow (Create Your Intel AMT Profiles on page 38).

In the Define the WiFi Profile dialog, do the following:

1. In the **WiFi profile name** field, enter a name for the WiFi profile. The setup name can be up to 32 characters, and must not contain ( / \ < > : ; * | ? ” ) characters.
2. In the **SSID** field, enter the Service Set Identifier (up to 32 characters) that identifies the specific WiFi network.
3. From the **Security type** drop-down list, select one of the following:
   - **WPAPSK**: Uses WiFi Protected Access key management protocol. Enter the **Security key** (passphrase) in the field provided (must contain between 8 and 63 printable ASCII characters).
   - **WPA2PSK**: Uses Robust Security Network (or WPA2) key management protocol. Enter the **Security key**(passphrase) in the field provided (must contain between 8 and 63 printable ASCII characters).
   - **WPAIEEE802_1**: Uses WiFi Protected Access key management protocol. Choose an existing 802.1X setup from the dropdown list.
   - **WPA2IEEE802_1**: Uses Robust Security Network (or WPA2) key management protocol. Choose an existing 802.1X setup from the dropdown list.
4. From the Encryption drop-down list, select one of the following:
   - Temporal Key Integrity Protocol (TKIP)
   - Counter mode CBC MAC Protocol (CCMP)

When a new setup is created, its priority value is one greater than the highest value of existing setups.

### 3.3.1.1 Editing and Deleting Wi-Fi Profiles

1. Select **Endpoint Groups** from the navigation bar at left, then select **Intel® AMT Profiles > Manage WiFi Profiles**.
2. Click the down-arrow next to the target Wi-Fi profile to edit or delete it. You cannot delete a network profile that is associated with an Intel AMT profile.

The Wi-Fi profiles are sorted in this list by their priorities, with the lowest priority number at the top of the list and the highest priority number, which will be used last, at the bottom of the list.

To change a profile’s priority, click the blue up and down arrow buttons to move a WiFi profile up or down.

## 3.3.2 Creating a New 802.1x Profile

The IEEE802.1x network protocol provides an authentication mechanism to devices wishing to attach to a LAN, either establishing a point-to-point connection or preventing it if authentication fails. It is used for most wireless 802.11 access points and is based on the Extensible Authentication Protocol (EAP). You can include the 802.1x profiles you define in the profile for wireless and wired connections.

If you do not plan to use 802.1X network protocol, you can skip this step.

**NOTES**

- 802.1x profiles require integration with Active Directory and an Enterprise-root CA.
- Be sure you understand your organization's network authentication requirements. If those are not met, Intel AMT may not function correctly. For example, some IT organizations have 802.1x access policies beyond requiring an AD computer object and valid 802.1x certificate, such as a passlist of allowed network hardware types.
- Information about configuring 802.1x authentication for Microsoft Active Directory (AD) Domain Services, including creating an AD Organizational Unit (OU) for use with 802.1x profiles, is available in the appendix of the Intel® EMA Server Installation and Maintenance Guide and the Intel® EMA Distributed Server Installation and Maintenance Guide. **If you plan to use 802.1x with AD Domain Services, ensure your Global Administrator performs the 802.1x for Active Directory configuration process described in this appendix before you create your 802.1x profile.**

### To Create a New 802.1X Profile:

Select **Endpoint Groups** from the navigation bar at left, then select **Intel® AMT Profiles > Manage 802.1x Profiles** and click **New Profile**. You can also create a new 802.1X profile as part of the Intel® AMT Profile creation workflow (Section 3.2). In the **Definition** dialog, do the following:

1. (Optional) Uncheck the **Enable** checkbox to disable this setup for wired connection.
2. Enter a **Name** for this 802.1x profile. The name can be up to 32 characters, and must not contain ( / \ < > : ; * | ? ” ) characters.
3. Choose either **EAP_TLS** or **EAP_PEAP_MSCHAP_V2** for **Protocol**.
4. Under **Active Directory**, enter the following information:
   - **Active Directory Organizational Unit (ADOU):** This is where the object will be stored in AD. The ADOU must be entered using the distinguished name format; for example, “OU=Out of Band Management,DC=vprodemo,DC=com”.
   - **Security Groups:** The AD Object created for the Intel AMT endpoint is by default automatically added to the AD Security group named “Domain Computers”. You can define additional Security groups to which the object will be added. For example, some RADIUS servers require objects to be members of a specific Security group. Use a new row for a new entry using the distinguished name format; for example: "CN=vPro8021XComputers,DC=VPRODEMO,DC=COM".

5. This step only applies to EAP_TLS. The **Client Authentication** portion of the screen is not displayed if you select **EAP_PEAP_MSCHAP_V2**. Under **Client Authentication**, for How to create the certificate, select the source of the certificate that will be installed in the Intel AMT endpoint. **From Microsoft CA** is recommended and the Intel® EMA server needs to be able to access the Microsoft CA.
   - From the **Certificate Authority** drop-down list, select the Enterprise CA that Intel® EMA will use to request a certificate that the RADIUS server can authenticate. This requires the Enterprise root CA to be configured to show it is a root certification authority via AD query. If you do not see the Enterprise root CA you wish to use, you will need to use the From the database option listed below.
   - From the **Server Certificate Template** drop-down list, select the template that will be used to create the client certificate. Refer to Intel AMT documentation for how to create valid template at the Certificate Authority Server.
   - Define the **Common Names** that will be included in the Subject Name of the generated certificate. For **Default**, the CN for Subject Name is User Principal Name, and the CNs for Subject Alternative Name are User Principal Name, DNS FQDN, Hostname, SAM Account Name, UUID of the new AD object representing Intel® AMT, Distinguished Name. For **User Defined**, select Common Names to be put into Subject Alternative Name and choose Subject Name. When Organization Unit is empty, Default is the only option available and the AMT hostname will be used as **CN for Subject Name**, no alternative names will be added.

     **NOTE**

     — You can select Distinguished Name to be included in the certificate's Subject Alternative Name, but Distinguished Name is not included in the **CN for Subject Name** drop-down list because it is not allowed in the certificate's Subject Name.

     The Subject Name will be used by the Intel AMT firmware as the Radius user name when connecting to an 802.1x network, so the Radius server must be configured to expect the Subject Name value as a valid user name.

   - **From database:** User can use a pre-uploaded certificate in the Intel® EMA database. Refer Upload Intel® AMT PKI Certificates on page 44 for how to uploading the certificate. Enter the target certificate thumbprint value to locate the certificate.
6. Under **Server Authentication – Trusted Root Certificate**, for **How to get the certificate**, select the source of the certificate that will be installed in the Intel AMT endpoint.
   - From the **Certificate Authority** drop-down list, select the Enterprise root CA that Intel® EMA will use.
   - **From the database:** User can use a pre-uploaded certificate in the Intel® EMA database. Refer Upload Intel® AMT PKI Certificates on page 44 for how to uploading the certificate. Enter the target certificate thumbprint value to locate the certificate.

7. Under **Advanced**, the **Available in S0** option is enabled by default, which allows Intel AMT to handle authentication to the Intel® EMA server in cases where an endpoint is in an S0 state but fails to authenticate to the server. Note that the Intel® EMA server still cannot access the endpoint until it authenticates successfully.
   - Disable (uncheck) this option only if you do not want Intel AMT to perform authentication to the Intel® EMA server with this profile.
   - For **PXE Timeout**, set the duration in seconds for which Intel AMT will hold an authenticated 802.1X session before timing out (range 0 - 86400 seconds, or one day). During the set duration, Intel AMT manages the 802.1X negotiation while a PXE boot takes place. After the timeout, control of the negotiation passes to the endpoint. This setting applies to Wired Connections.
8. Under **Radius Server Validation**, select one of the following to specify how you want Intel AMT to verify the Subject Name in the certificate provided by the RADIUS AAA server.
   - Do not verify
   - Verify using FQDN
   - Verify using Domain Suffix

### 3.3.2.1 Editing and Deleting 802.1X Profiles

1. Select **Endpoint Groups** from the navigation bar at left, then select **Intel® AMT Profiles > Manage 802.1x Profiles**.
2. Click the down-arrow next to the target profile to edit or delete it. You cannot delete a network profile that is associated with an Intel AMT profile.

## 3.4 Create Your Intel AMT Profiles

**Roles**: Tenant Administrator, Endpoint Group Creator

If you plan to use Out-of-Band (OOB) features to manage your endpoints (i.e., endpoint management features that work when the endpoint's operating system is unavailable), you must configure Intel® AMT on your endpoints. You can manually configure Intel AMT on each and every endpoint, or you can have Intel® EMA set up Intel AMT on all your endpoints automatically. In order for Intel® EMA to automatically set up Intel AMT, you must configure at least one Intel AMT profile for Intel® EMA to use.

If you do not want to use Intel AMT auto-setup, you do not need to configure Intel AMT profiles and can skip this step.

**To create a new Intel® AMT profile:**

1. From the navigation bar at left, select **Endpoint Groups**, then click the **Intel AMT Profiles** tab.
2. Click **New Intel AMT Profile**, fill out the fields for each section of the new Intel AMT Profile (General, Power States, etc.) , and click **Save**. These sections are described in detail in the following subsections.
3. If you are performing an initial Tenant setup, after completing each section of the Intel AMT profile and clicking **Save**, proceed to Upload Intel® AMT PKI Certificates on page 44 to upload Intel AMT PKI certificates before enabling Intel AMT autosetup.

### 3.4.1 General Settings

Enter a **Profile Name** and **Profile Description**, then specify how Intel® EMA server will communicate with the endpoint's Intel AMT (CIRA or TLS Relay). Refer In-band vs. Out-of-band on page 15 for more information about CIRA and TLS.

- **Always Use Intel AMT CIRA** - This option sets a random CIRA home domain. CIRA will always be used (no TLS Relay).
- **Use Intel AMT CIRA unless on a specified network** - Displays the CIRA home domain and allows you to enter another domain. If the specified domain is detected, TLS Relay is used.
- **Use TLS Relay** - Uses TLS Relay only (no CIRA).

**NOTE**

If you specify CIRA,

- Intel® EMA uses a self-signed certificate for CIRA communication.
- You must define an intranet suffix. When the Intel AMT endpoint is at the network matching the defined intranet suffix, Intel AMT will stop CIRA and use TLS Relay instead.

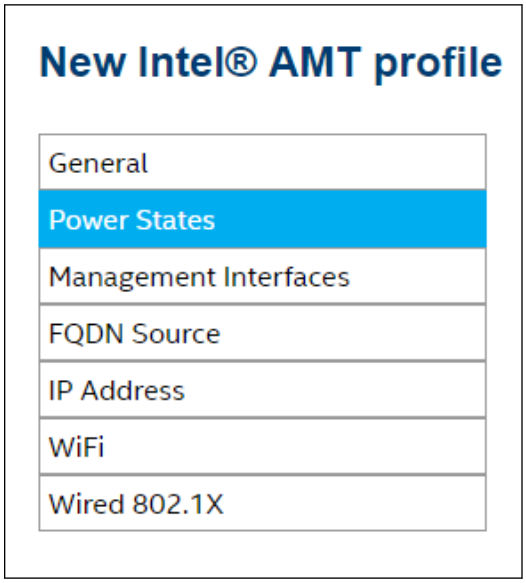
**NOTE**

To force Intel AMT to always open a CIRA tunnel, enter a fake domain suffix in the CIRA intranet suffix field under General settings when creating your Intel AMT profile. This fake domain suffix should be complex enough to prevent anyone from guessing it and thus using it to prevent a CIRA connection and open local management ports. If viewing a profile created with a previous version of Intel® EMA, you will see a domain suffix auto-filled here.

If you specify either of the above settings,

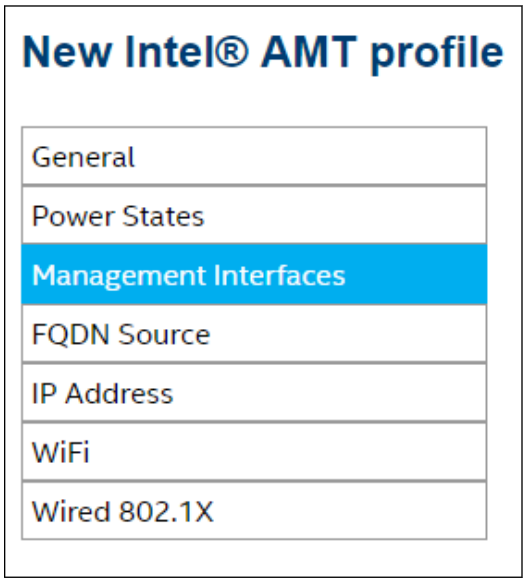
- For endpoints with Intel AMT 12 or later, you have the option to add proxies used for Intel AMT to connect to Intel® EMA server.

### 3.4.2 Power State Settings




The default, and the recommended choice, is "Any time the system is connected to power through all system power state (S0 – S5)".

### 3.4.3 Management Interface Settings



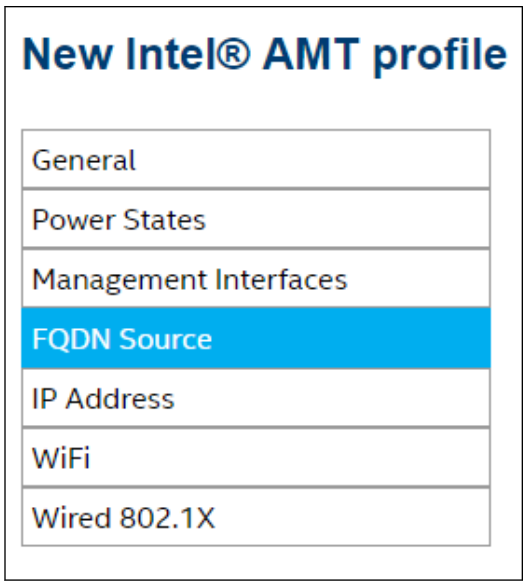

Select the interfaces you want to be able to open on the endpoints:

- **KVM redirection** – Opens the Keyboard/Video/Mouse (KVM) Redirection interface, which allows you to interact with the endpoint as if your keyboard, video, and mouse were physically connected to that system.
- **User Consent** - Presents the target endpoint's user with a consent code to allow remote management interaction with the endpoint. Choose either KVM or KVM + Advanced Boot Options (for use when remotely performing advanced boot operations such as USBR or Remote Secure Erase). If either is selected, you will be prompted to enter the consent code provided by the endpoint's user when connecting via KVM or attempting to perform advanced boot operations. If the endpoint is in Client Control Mode, user consent is enforced regardless of options selected here. You can also modify the timeout period in seconds.
- **Web-based user interface** – Enables you to manage and maintain Intel® AMT systems using a browser-based interface.
- **Serial over LAN** – Enables you to remotely manage Intel AMT systems by encapsulating keystrokes and character display data in a TCP/IP stream.
- **IDE/USB redirection** – IDER enables you to map a drive on the Intel AMT system to a remote image or drive. This functionality is generally used to reboot an Intel AMT system from an alternate drive. USBR enables you to map a drive on the Intel AMT system to a remote image or drive. In contrast to IDER, which presents remote floppy or CD drives as though they were

integrated in the host machine, USBR presents remote drives as though they were connected via a USB port.

- **OCR (One Click Recovery)** - Initiates recovery process to return specified endpoint's OS to a last known good state in a secure manner. Uses Intel AMT Out-of-Band (OOB) connectivity.
- **RPE (Remote Platform Erase)** - Initiates process to remotely erase all platform information, including (optionally) the platform's Intel AMT information in a secure manner. Uses Intel AMT Out-of-Band (OOB) connectivity.

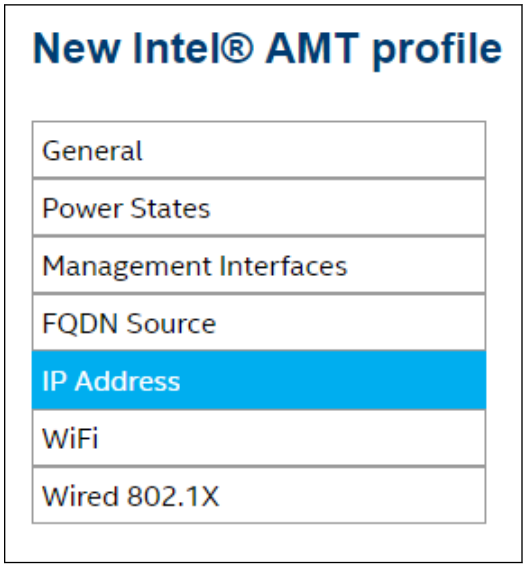
### 3.4.4 FQDN Settings




Select how the host name and the domain suffix will be set on Intel AMT.

- **Shared with host OS**: The host name is the host name from OS. The domain suffix is blank.
- **On-board connection-specific DNS**: The host name is the host name from OS. The domain suffix is the "connection-specific DNS suffix" of the on-board wired LAN interface.
- **DNS lookup**: Uses the values returned by dnslookup on the IP address of the on-board wired LAN interface. This option requires the DNS be configured correctly with reverse lookup zones.
- **Primary DNS**: Both the host name of the domain suffix (primary DNS suffix) are from OS.

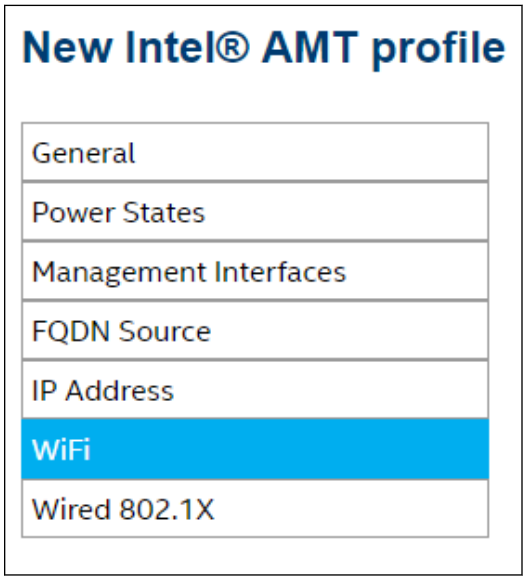
### 3.4.5 IP Address Settings




Select how Intel AMT will get the IP address of the endpoint (host).

- **From the DHCP server** - Use this when the host is assigned an IP address automatically from DHCP.
- **Use a static IP address from host** - Use this when the host has a statically assigned IP address.

### 3.4.6 Wi-Fi Settings




Choose from the following options:

- **Allow WiFi connection without a WiFi profile** – Select this option if you want to allow WiFi connection without a WiFi setup (using the hosts WiFi settings).
- **Use the selected WiFi profiles** – Select this option if you want to define WiFi setups. The total number of WiFi setups that can be configured depends on the version of Intel AMT. Refer Creating a New Wi-Fi Profile on page 35 for more details.

Intel AMT includes a Wireless Profile Synchronization feature. This feature enables synchronization of the wireless profiles in the operating system with the WiFi setups defined in the Intel AMT endpoint. When the **Synchronize with host platform WiFi profiles** check box is selected, support for this feature is enabled. To use this feature to synchronize profiles, the Intel Management Engine (Intel ME) components must be installed on the endpoint. Refer to the endpoint's OEM for these drivers.

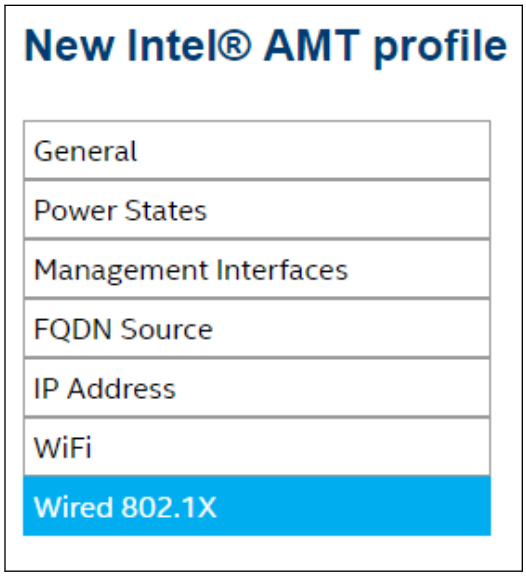
*Note:* Although the host platform's administrator can specify up to 16 preconfigured WiFi profiles, Intel AMT will only synchronize up to 8 profiles. Therefore, if all 8 profiles are currently synched and a new WiFi profile is added on the host, the oldest synched profile in Intel® EMA will be replaced by the new one.

By default, connection to the Intel AMT endpoint via the WiFi connection is available only when the operating system is in the S0 power state. If you want to enable the WiFi connection in all S0-S5 power states, select **Enable WiFi connection in all system power states (S1-S5)**.

To enable the One Click Recovery (OCR) feature to work wirelessly, select **Enable WiFi profile sharing with UEFI BIOS**. For more information on OCR, refer One Click Recovery on page 20

To create a new WiFi profile, click **New...** and complete the Define the WiFi profile dialog, as described in Creating a New Wi-Fi Profile on page 35.

### 3.4.7 Wired 802.1x Settings




Choose an existing 802.1X setup to use for wired networking. Refer Creating a New 802.1x Profile on page 36 for more details.

To create a new 802.1X profile, click New… and complete the Define the 802.1x profile dialog, as described in Creating a New 802.1x Profile on page 36.

## 3.5 Upload Certificates

**Roles**: Tenant Administrator

This section describes how to upload various certificates, including Enterprise Root Certificates and Intel AMT PKI certificates.

**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.
2. Click **Upload**.
3. The Certificate dialog is displayed.
4. Enter the **Entry Name** then click **Choose File**. Certificate files ending in .CER do not require a Password. Certificate files ending in .PFX require a Password. Note that the certificate file to be uploaded must be less than 1MB.
5. In the Certificate dialog, click **Upload**.

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 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.

If you are performing an initial Tenant setup, proceed to Enable Intel AMT Auto-Setup on page 46 to enable Intel AMT autosetup.

### 3.5.1 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 configuration of user consent requirements. 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 file needs to have the full certificate chain. Also, it needs to be issued with the supported OID 2.16.840.1.113741.1.2.3 (this is the unique Intel AMT OID).

**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. Refer section below for details.

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 and includes the private key. 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 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.

  Refer Troubleshooting in Appendix: Troubleshooting on page 77 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.

Refer Upload Certificates on page 43 for steps to upload certificates.

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.

If you are performing an initial Tenant setup, proceed to Enable Intel AMT Auto-Setup on page 46 to enable Intel AMT autosetup.

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

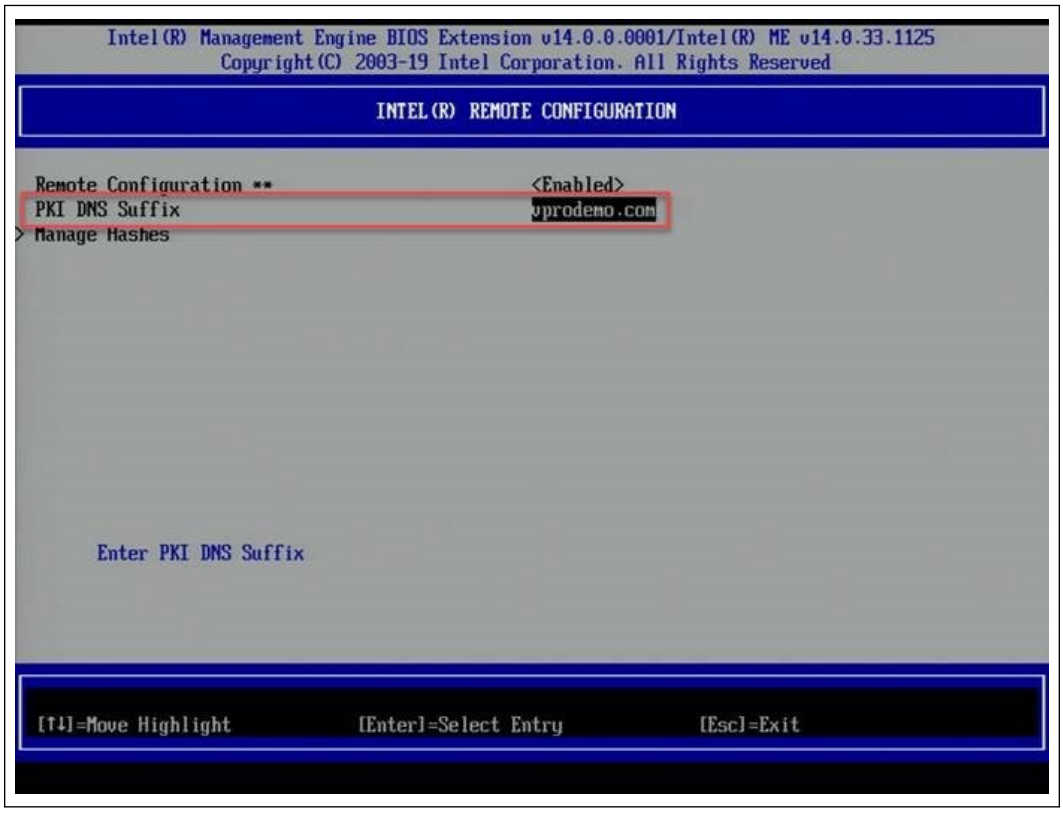
This procedure is required in order to configure Intel AMT in Admin Control Mode (ACM) on LAN-less endpoints. For LAN-less devices, there currently is no way for Intel AMT to determine that it is on the same domain as the PKI certificate's DNS suffix. Therefore, in order to configure a LAN-less endpoint's 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 7. 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.

## 3.6 Enable Intel AMT Auto-Setup

**Roles:** Tenant Administrator, Endpoint Group Creator, and Endpoint Group User[†]

[†] With appropriate access permissions for this group

**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 agent first connects if the Intel AMT auto-setup was defined before deploying the agent.

**NOTE**

- Using an auto-setup profile on an endpoint already provisioned in CCM systems (even if provisioned by another tool), the auto provisioning flow will "adopt" the endpoint into your Intel® EMA instance.

**To enable auto-setup:**

1. From the navigation bar at left, select **Endpoint Groups,** then click the down-arrow 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. Refer Upload Intel® AMT PKI Certificates on page 44 for more information about PKI certificates. Refer ChapterIn-band vs. Out-of-band on page 15 and Intel® AMT Provisioning/Setup Flow in Intel® EMA on page 16 for more details about the activation methods .
5. If you deselect the Randomize checkbox (selected by default), you must 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. It is recommended that you use a random administrator password on all endpoints so that if one endpoint's administrator password is compromised the other endpoints are not compromised as well. If necessary, you can retrieve the random password for an endpoint using the Intel® EMA API. For more information, see the and the online API details available by going to https://www.intel.com/content/www/us/en/support/articles/000055621/software/manageability-products.html, clicking **Detailed HTML API Documentation**, and opening the downloaded file **Vxswagger.html** in a browser.
6. If using TLS-PKI activation method, 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. Again, you can use the Intel® EMA API to retrieve the random password if necessary. This action is not displayed if using host based provisioning.
7. Select a certificate from **Available Certificates** (if any are available).
8. Click **Save**.
9. If you are performing an initial Tenant setup, proceed to Deploying the Agent to Your Endpoints on page 49 to deploy the agent files to your endpoints.

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.

If the administrator password is changed from random to specified password, specified password to random password, or specified password to an updated specified password, the password for the admin account for the endpoint system will be updated.

# 4.0 Deploying the Agent to Your Endpoints

**Roles**: Not applicable; not specific to any Intel® EMA user roles This section describes how to manually install the Intel® EMA Agent on a target endpoint system. This procedure is also applicable for those who want to set up a scripted mass-deployment of the Intel® EMA Agent to a large number of endpoint systems.

**Endpoint Host Names**: Beginning with Intel® EMA 1.12.0 endpoint host names support Unicode characters. Previous versions of Intel® EMA only support ASCII characters for host names.

The two agent files you created in Create Agent Files for Deployment to Managed Endpoints on page 33 , **EMAAgent.exe** and **EMAAgent.msh**, must be copied to each endpoint system that you want to manage with Intel® EMA. You can manually copy them to the endpoint systems or use a mass deployment tool. Either way, these two files must be located in the same folder on the endpoint system(s) and must have the same filename pre-fix (i.e., EMAAgent).

**NOTE**

For information about installing the Intel® EMA Agent as a console, refer Appendix - Intel® EMA Agent Console on page 91.

The following table describes the properties of each of these files.

**Table 1. Intel® EMA Agent Files**

| File Name | Description |
|---|---|
| EmaAgent.exe | This is the Agent's installation file. You must execute this file with administrative privileges to install/update/uninstall any instance. |
| EmaAgent.msh | This is the policy file. This file determines which Endpoint Group the endpoint will belong to and enables the Intel® EMA Agent to contact the Intel® EMA server. |

**NOTE**

The Intel® EMA Agent is not designed to run in a VM on the target endpoint, even on the Base Hypervisor. The LAN/WLAN cannot interpret multiple IP addresses correctly. No Hypervisor has been written to accommodate the address translation required to use Intel AMT. This affects the agent's ability to connect to Intel AMT and perform Out of Band (OOB) actions on the endpoint. It is possible that in-band actions may work in this scenario, but that is not certain.

### To Install on an Endpoint System:

1. Copy the two agent files, EMAAgent.exe and EMAAgent.msh, from the Downloads folder on the system on which they were created to the target endpoint system. Be sure to place the two files in the same folder.

2. On the endpoint system, open a command window (cmd.exe) with administrator rights and go to the folder where the two agent files are located.
3. Run the following command to install Intel® EMA Agent.

```
EmaAgent.exe -fullinstall
```

**NOTE**

If you want the Agent to be able to access a proxy network, you must configure a proxy for the Agent on that endpoint. Proxy Configuration on page 51

### To Uninstall:

```
EmaAgent.exe -fulluninstall
```

### To View Help for the Agent Installer:

```
EmaAgent.exe -?
```

**NOTE**

The agent installer can also be run as a GUI by right-clicking on the EmaAgent.exe file in Windows Explorer and selecting Run as Administrator. In the Installer dialog, click Install/Update.

For installation verification and troubleshooting information, refer Verifying and Troubleshooting Agent Installation on page 51.

## 4.1 Install Directory

The default installation directory for the Win64 Service is C:\Program Files\Intel\Ema Agent.

Both services will include the following files:

- EmaAgent.exe: Executable service file.
- EmaAgent.log: Used for local logging.
- EmaAgent.msh: Installed policy file.
- mesh.db: The Intel® EMA agent database.

## 4.2 Intel® EMA Agent Database

Once the Agent service is installed, a local database is generated to save settings and certificates. The database is stored in the same path as the agent's running executable binary.

## 4.3 Windows Service Information

After the Agent is installed as a Windows service, you can access it by using the Windows Service Manager.

1. Open the **Run** window by pressing the Windows key plus the R key, at the same time.
2. Type **services.msc** in the **Run** window.
3. Press the **Enter** key.
4. This displays all the installed services in Windows.
5. To find the Agent service, look for the **Intel(R) EMA Agent background service** name.
6. Select the Agent service and check if it's running correctly.
7. At this point, you can stop or restart the service if you wish to. If the service is already stopped, you can start it.

## 4.4 Proxy Configuration

If you want the Agent on an endpoint to be able to access a proxy network, you must configure a proxy for the Agent on that endpoint.

To install the Agent on an endpoint and specify a proxy at the same time, use the following command on the target endpoint:

```
EmaAgent.exe -fullinstall -proxy:<address>:<port>
```

The Agent creates a file named **EmaAgent.proxy** in the installed directory on the endpoint, where it stores the value of the HTTPS proxy you specified.

If you do not use the -proxy parameter when you run the installer, then whatever Windows proxy settings are currently configured in the Windows Control Panel's LAN Settings dialog for the user that you are logged in as when you run the installer will be applied to the Agent (i.e., stored in the EmaAgent.proxy file).

**NOTE**

**Automatic configuration** settings (i.e., the top half of LAN Settings dialog) are not handled by Intel® EMA; only the **Proxy server** (lower half) settings are stored.

## 4.5 Verifying and Troubleshooting Agent Installation

You can use the Intel® EMA Agent's command line interface to display information about the connection to the Intel® EMA server. Perform the following steps on the endpoint on which the agent is installed.

1. Open a command prompt window as Administrator.
2. Change directory to the Intel® EMA Agent installation directory (refer section 1.1).
3. Execute one of the commands below.

### To Test if Agent is Running

Command:

```
tasklist /fi "imagename eq EmaAgent.exe"
```

Example (success):

```
λ tasklist /fi "imagename eq EmaAgent.exe"
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
EmaAgent.exe                 15396 Services                   0     42,816 K
```

Example (failure):

```
λ tasklist /fi "imagename eq EmaAgent.exe"
```

```
INFO: No tasks are running which match the specified criteria.
```

### To Test if Agent is Connected

Command:

```
netstat -nao | find "8080"
```

Example (success):

```
EMAAgent.exe -swarmserver
```

```
TCP  <agent IP>:<random port> <swarm server IP>:8080  ESTABLISHED     <process ID>
```

```
TCP 192.168.1.100:51662  192.168.0.18:8080 15396
```

Example (failure):

```
λ netstat -nao | find "8080"
(returns empty results)
```

### To Obtain Swarm Server Name

Command:

```
EMAAgent.exe -swarmserver
```

Example (success):

```
EMAAgent.exe -swarmserver
Intel(R) EMA Swarm server address and port are 192.168.0.18:8080
```

Example (failure):

```
EMAAgent.exe -swarmserver
Unable to read Intel(R) EMA Agent database.
```

### To Obtain Agent Node ID

Command:

```
EMAAgent.exe -nodeidhex
```

Example (success):

```
λ EMAAgent.exe -nodeidhex
Intel(R) EMA Agent node is: <HEX ID>
```

Example (failure):

```
λ EMAAgent.exe -nodeidhex
Not defined, start the Intel(R) EMA Agent to create a nodeid.
```

### To Obtain Proxy Server Information

Command:

```
EMAAgent.exe -agentproxy
```

Example (success):

```
ComputerName     : <ema-fqdn>
RemoteAddress    : <server IP address>
RemotePort       : 8080
InterfaceAlias   : Ethernet 2
SourceAddress    : <client IP address>
TcpTestSucceeded : True
```

Example (failure):

```
ComputerName           : <ema-fqdn>
RemoteAddress          : <server IP address>
RemotePort             : 8080
InterfaceAlias         : Ethernet 2
SourceAddress          : <client IP address>
PingSucceeded          : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded       : False
```

### To Test if Intel® EMA Server is Reachable

Command:

```
powershell.exe test-netconnection -computername <ema-fqdn> -port 8080
```

**NOTE**

The connection tests above apply to endpoints belonging to endpoint groups created before updating to Intel® EMA 1.15.0. For endpoints in endpoint groups created after the update, repeat all tests using port 8081 instead of port 8080.

Example (success):

```
ComputerName     : <ema-fqdn>
RemoteAddress    : <server IP address>
RemotePort       : 8080
InterfaceAlias   : Ethernet 2
SourceAddress    : <client IP address>
TcpTestSucceeded : True
```

Example (failure)

```
ComputerName           : <ema-fqdn>
RemoteAddress          : <server IP address>
RemotePort             : 8080
InterfaceAlias         : Ethernet 2
SourceAddress          : <client IP address>
PingSucceeded          : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded       : False
```

# 5.0 Managing Users and User Groups

Depending on the size and complexity of your organization, you may decide you need additional users to help manage your endpoints (refer User Roles on page 11 for information on user roles).

In order for users to manage endpoints in an Endpoint Group, the users must be assigned to the same User Group as the Endpoint Group they are to manage (User Groups on page 12).

## 5.1 Adding, Modifying, and Deleting Users

**Roles**: Tenant Administrator, Account Manager, Global Administrator

1. Select **Users** on the left-hand navigation strip (or click **Add or remove users** under **Users** on the Overview page).
2. To add a user, click **New User....**
3. Enter user information and click **Save**.
4. To add the new user to a User Group, click the down-arrow next to the new user and select **Group memberships**, then select the groups to which this user should belong.

**NOTES**

- To change the password for your own user account, you must enter your current password first. If you are editing other accounts (that your role can manage), you do not need to enter the user's current password.
- For "locked" users, click the down-arrow and edit the user to unlock the account.
- If a Client Credentials account has been created in this Tenant, you may see a user with the role of Tenant Administrator listed and a user name format that is not in email account form (i.e., user@domain.com). For information about Client Credentials accounts, refer Appendix - Performing Intel® EMA Endpoint Operations from a Machine-to-Machine Client Application on page 95.
- If you configured Intel® EMA to use Active Directory authentication, ensure the username of any user you create corresponds to the userPrincipalName attribute of the Active Directory user. The Password field is not shown or needed in this mode.
- If you configured Intel® EMA to use Azure AD for SAML authentication, you cannot delete the initial account that you created during installation, nor can you edit the role for this account. You can, however, edit the password for the initial account. Furthermore, for Azure AD ensure the username of any user you create matches the Universal Principle Name (UPN) of the Azure AD user. The password field is not shown or needed in this mode.
- If you have configured Intel® EMA to use normal (username/password) authentication, when creating a new user or while updating the password for an existing user, the password will be checked based on the password policy. The password policy can be configured by the global admin using **Settings** in the **Security Settings**. By default the password policy will require min length 8, max length 255, require complexity (uppercase/lowercase/number/special character) and will be checked against a disallowed password list.

To edit or delete an existing user, click the down-arrow next that user and select **Edit** or **Delete**.

## 5.2 Creating New User Groups

**Roles**: Tenant Administrator, Account Manager, Global Administrator

1. Select **Users** on the left-hand navigation bar, then click the **User Groups** tab.
2. Select the **User Groups** tab, then click **New Group** and enter a **Group Name** and **Description** and select the access permissions to grant to the users in this User Group.

   **NOTES**

   - The **New Group b**utton will be disabled (grayed out) if you have not created at least one Tenant yet (Global Administrator only).
   - **Description** is a required field and you will not be able to save the group until a value for it is provided.

3. Click **Members** and select the users to add to this User Group (or you can do this later when you create a new user).

4. (not available to Global Administrator) Click **Endpoint Groups** and select the Endpoint Groups to which this User Group will have access.

To edit or delete an existing User Group, click the down-arrow next that group and select **Edit** or **Delete**. If you delete a User Group, the users and endpoints associated with that group are not affected.

## 5.3 Assigning Endpoint Groups to User Groups

**Roles:**Tenant Administrator, Endpoint Group Creator, with appropriate access permissions for this group

As described in User Groups on page 12, User Groups are used to manage user access to Endpoint Groups, and thus to the endpoints themselves. In order for a user to perform management tasks on the endpoints in a particular Endpoint Group, the user and the Endpoint Group must belong to the same User Group.

- Select **Users** on the left-hand navigation bar, then click the **User Groups** tab.
- Click the down-arrow for the target User Group and select **Assign Endpoint Groups**.
- In the dialog box, select the target Endpoint Groups and their associated rights, then click **Save**.

## 5.4 Managing Active Directory User Groups

Active Directory (AD) user groups allow AD user accounts to access Intel® EMA without having to add them individually. These user groups can be configured to have the capabilities of any available user role.

To add a new EMA user group based on an AD group:

1. Go to **Intel® EMA users** > **AD User Groups** > **New group**
2. You will require the AD Distinguished Name (DN) to link those users to Intel® EMA. Select the role for those users and for roles **Endpoint Group User** and **Endpoint Group Creator**, assign specific granular access to Intel® EMA features. You can later edit the role and the granular access permissions by using the **Edit** function.
3. To link the existing Endpoint Groups to the new Intel® EMA AD User group, go to **Endpoint Groups** tab.
4. After selecting least one Endpoint Group from the available list, click **Save** to complete. You can later edit the Endpoint Groups your new Intel® EMA AD User group through the Edit function.

This functionality, allow to create an Intel® EMA User group based on the same users as the AD group of your selection.

**NOTES**

- This option is only available for instances using Windows* or Entra ID credentials..
  - For Entra ID credentials, make sure you grant **"GroupMember.Read.All"** and **"User.Read.All"** permissions to your Intel® EMA application.
- You will require the Distinguished Name of the AD group to safely identify the AD group you want to link.
  - You may need to contact the Active Directory Administrator to get the necessary information
- The access and permissions you select upon group creation, will apply to all user in that AD group.
  - Users who are part of more than one Intel® EMA AD User group, will inherit the highest level of access granted by any of those Intel® EMA AD User Groups.
- Users will be added to EMA as they log in to the application using their Windows credentials. The same way, users removed from AD will lose access to EMA once they try to log back in.
- If the AD Group is renamed in Active directory, We recommend to first delete the Intel® EMA AD User Group with the old name and add a new Intel® EMA AD User with the new name. This will migrate all active users into the new EMA user group. If you fail to add a new group linked to the new name, users in the group with the old name might lose access to Intel® EMA.

## 5.5 Managing SAML Authentication Users

You can add EMA Users for SAML SSO login. User accounts in your SAML Provider must use the same email addresses as their corresponding EMA User accounts. The new user must match with the Identity provider user's UPN in a valid email format. Our system will use the first available non-empty value in email format from the following claims, in this order: nameidentifier, upn, emailaddress and name. You can also add them to any groups memberships for more info on adding the users, follow the steps in Adding, Modifying, and Deleting Users on page 55.

# 6.0 Managing Your Endpoints

**Roles:** Tenant Administrator, Endpoint Group Creator (based on group and rights), Endpoint Group User (based on group and rights).

Once you've set up your Tenant(s) to reflect the structure of your organization, you are ready to start using Intel® EMA to manage your endpoint systems.

## 6.1 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. Refer Intel® AMT Provisioning/Setup Flow in Intel® EMA on page 16 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 (to unprovision, use the **Remove provisioning** button as shown in Figure below.

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. Refer Chapter 1 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. Refer 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. Refer Setting or Verifying the Correct PKI DNS Suffix in Intel® MEBX on page 45for more information on LAN-less systems.

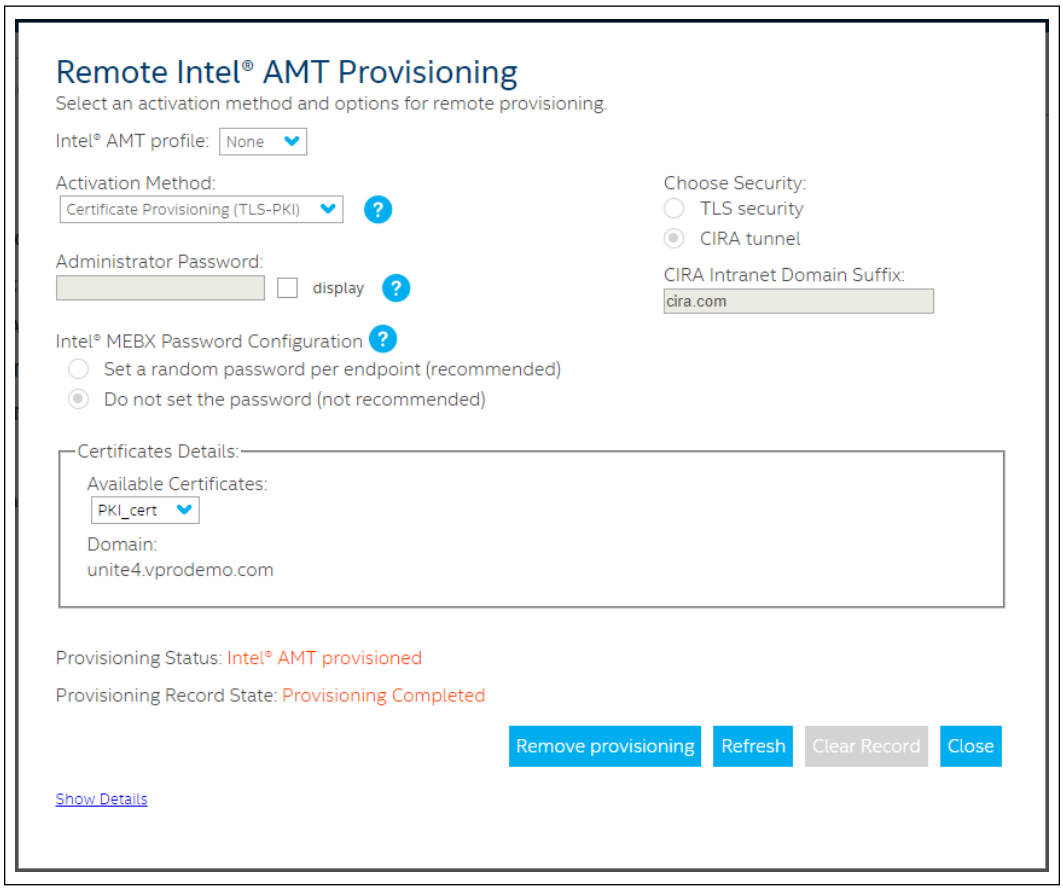
For CIRA or TLS Relay, Refer In-band vs. Out-of-band on page 15 for details.

**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 8. Provision Intel® AMT On-demand**




## 6.2 Intel® EMA Agent

The Intel® EMA Agent connects to the Intel® EMA server via TCP and port 8080 for end point groups created before updating to Intel® EMA version 1.15.0, and port 8081 for endpoint groups created after updating to that version. When Intel® EMA Agent is installed, it will set up the following Windows Firewall in-bound rules for the installed agent binary process. If you are using a different firewall, make sure that the following in-bound rules are set for the installed agent binary process:

- Peer-to-peer traffic: UDP with local port at 16990, any IP for local and remote addresses, and edge traversal blocked.
- Peer-to-peer traffic: TCP with local port at 16990, any IP for local and remote addresses, and edge traversal blocked.
- Local loopback management traffic: TCP with local port at 16991, 127.0.0.1 for local and remote addresses, and edge traversal blocked.

For information about troubleshooting the Intel® EMA Agent, refer Verifying and Troubleshooting Agent Installation on page 51.

### 6.2.1 Agent Windows Registry Information

Registry keys created by the Agent's installation depend on the architecture of the Microsoft Windows OS and the Intel® EMA Agent (console and service). These are the registry paths for Intel® EMA Agent by architecture:

- Win64 Service:

  HKEY_LOCAL_MACHINE -> "Software\Intel\EmaAgent"
- Win64 Console:

  HKEY_CURRENT_USER -> "Software\Intel\EmaAgent"

The following registry keys should exist at this reg key root when the Intel® EMA Agent is installed/running:

- **MeshId** - REG_SZ that contains the Endpoint Group ID from the MSH file; if no MSH file is present, then this value will be empty.
- **MeshName** - REG_SZ that contains the Endpoint Group Name from the MSH file; if no MSH file is present, then this value will be empty.
- **NodeId** - REG_SZ that contains the Endpoint ID.

  **NOTE**

  Endpoint ID is tied to the Agent root certificate. Different root certificates are used for service/console.

- **Version** - REG_DWORD that contains the version number of the running EmaAgent.
- **EnhancedLoggingLevel** - REG_DWORD that contains the logging level. By default this is set to 3, which disables enhanced debug logging. To enable enhanced debug logging, edit the registry and set EnhancedLoggingLevel to 4.

## 6.3 Viewing Your Endpoints

Tenant administrators, endpoint group creators, and endpoint group users can see the endpoints to which they have access (with the appropriate access permissions) on the **Managed Endpoints** page.

Select **Endpoints** from the navigation bar at left, then select the **Managed Endpoints** tab.

If you are currently managing 1000 or less endpoints, they will be loaded for display automatically. If you have more than 1000 managed endpoints, click the **Load all Endpoints** button to view all currently managed endpoints. This may take several minutes.

You can also enter a search criteria in the Search field to search for endpoints that match the specified criteria.

Once results are displayed, a **Filter** panel appears at left. To filter results, select the desired filter criteria.

**NOTE**

The **Connection** status shown is the in-band connection status.

For more information about a particular endpoint, click **View** for an endpoint in the list to access its information page. The tabs on this page are described in the following subsections.

### 6.3.1 General Tab

Displays general information about the selected endpoint.

**NOTES**

- The **Manage this endpoint** drop-down menu options are described in Section *Performing Actions on Endpoints*.
- Connected status is for in-band connection.
- Once the endpoint's Intel® AMT firmware has been set up/provisioned by Intel® EMA, if the Web based user interface has been enabled in the Intel AMT Profile Management Interface Settings, the "Device Page" link will be enabled to access the Intel AMT default web interface on that endpoint. If the Web based user interface has not been enabled, the "Device Page" link will not be shown.
- Intel Manageability Engine (Intel ME) version and setup status is shown on this page. If Intel ME is set up but Intel® EMA does not have the setup record, a warning will be displayed.

### 6.3.2 Hardware Manageability Tab

Allows you to perform many out-of-band Intel® AMT operations. In order for this to work, Intel AMT must be configured by the current Intel® EMA instance. That is, endpoints configured by a different Intel® EMA instances cannot be operated on using this tab.

Select an action to perform from the list of actions in the left-hand pane.

**NOTES**

- Do not change any Intel AMT settings using this tab. Doing so can result in a loss of manageability for the endpoint.
- This tab integrates Intel® Manageability Commander (Intel® MC) into the Intel® EMA user interface. Actions on this tab are performed via Intel MC. For information about the actions available in the list, see the Intel MC user documentation available at the link below. https://downloadmirror.intel.com/27807/Intel%20Manageability%20Commander%20User%20Guide.pdf
- The IP address of an endpoint provisioned for CIRA will be reported as **unknown** on the Hardware Manageability tab. However, on the Intel AMT webpage, the IP address of that endpoint will be reported as **0.0.0.0**.
- If the endpoint is using Modern Standby, then in order to successfully wake from Modern Standby the endpoint must have the Intel HID (Human Interface Driver) Event Filter device driver installed and a BIOS with Intel Proprietary Wake implemented. Alternatively, connecting via Remote Desktop and using the mouse/keyboard will also wake a system from Modern Standby.

## 6.3.3 Desktop Tab

Allows you to change the following settings using in-band remote KVM functionality:

| | |
|---|---|
| | Disconnects the current in-band KVM session. |
| Select display | If the endpoint has multiple displays, you can choose the target display you want to see. |
| Scale | Adjust the scale percentage of screen render resolution. A smaller value means more resolution reduction. You will get the best result if you use 50% (half) or 100% (full scale). |
| Quality | Adjust the level of bitmap compression. A smaller value means more compression, but with reduced resolution. |
| | Rotate the rendered display on Intel® EMA. This is useful when the target endpoint display is in Portrait mode. |
| | Paste plain text from console system's clipboard (i.e., the computer running the Intel® EMA web-based UI) to the current target endpoint via in-band KVM. |

***continued...***

| | |
|---|---|
| | *Notes:* • Before using the Paste from Clipboard feature, you must give your browser permission to access the clipboard. For Internet Explorer and Chrome, you will be automatically prompted the first time you click the Paste icon. For Firefox, you must manually update the Preferences in Firefox to set the following to True: **dom.events.asyncClipboard**, and **dom.events.testing.asyncClipboard**.<br>• :If you notice unexpected characters or case in the pasted output on the target endpoint, Refer "Appendix: Troubleshooting" under the topic "In-band KVM paste from clipboard results in unexpected characters or case". |
| Ctrl + Alt + Del | Send the "Ctrl + Alt + Del" key combination. Several special key combinations get intercepted by the Windows operating system the web browser is running on. Use this option to send a "Ctrl + Alt + Del" to the remote system. |
| | Expand KVM to full screen. This uses the web browser's full screen API to expand the remote KVM to full screen mode. To exit this mode, use web browser's in-box control (e.g., Esc key). |

This tab will be disabled if any of the following are true:

- The endpoint group policy does not allow this action
- The endpoint is not in-band connected to Intel® EMA
- The logged-in user does not have appropriate access permissions to the endpoint

**NOTES**

- User consent for in-band KVM will impact the behavior of this feature. Refer Creating New Endpoint Groups on page 31 for details.
- When the in-band KVM session is first started, it will display the contents of all the monitors connected to the endpoint.
- In Intel® EMA versions before 1.12.0, events such as Windows displaying a UAC prompt or logging out of Windows, would cause all displays to be shown. Intel® EMA 1.12.0 and later will maintain the display selection when these events occur.
  - If you are viewing the non-primary display in Windows when one of these events occurs, you may see a black screen and need to switch to the primary display using the display selection drop-down menu.
- If the display you have selected becomes unavailable during your in-band KVM remote control session, Intel® EMA will default to showing all available displays in the remote control window.
- Note the following for situations in which multiple users (i.e., web browsers) connect to the same endpoint's KVM:
  - User consent will not be requested again if the previous consent request is still active.
  - All sessions will compete with the mouse and keyboard input
  - The scale, bitmap quality, and display selection will impact all sessions
  - The rotation will only impact the current browser

### 6.3.4 Terminal Tab

Provides both in-band and out-of-band remote terminal functionality. Only text-based commands are supported.

This tab will be disabled if any of the following are true:

- The endpoint group policy does not allow this action.
- The logged-in user does not have appropriate access permissions to the endpoint
- If the endpoint is not provisioned, and the endpoint is not in-band connected to Intel® EMA

The "Intel® AMT terminal" is a Serial-Over-LAN (SOL) terminal. If interacting with the endpoint's BIOS, the BIOS must be the text-versioned BIOS.

Click the **Actions** menu and choose from the following options:

- **Start Terminal** - Use for endpoints that do not have Intel AMT configured. In band.
- **Start Intel AMT Terminal** - Disabled if endpoint is not provisioned. Use to interact with SOL tools and applications other than BIOS (for example, Windows PowerShell) on endpoints that have Intel AMT configured.
- **Boot to BIOS** - Disabled if endpoint is not provisioned. Use to boot an endpoint with Intel AMT configured to its text-versioned BIOS and then interact with the BIOS once booted. Note that the endpoint's BIOS must support this feature. Also, how the BIOS is presented may vary depending on individual BIOS implementations. The information that is displayed is coming from the endpoint's BIOS, and depending on the BIOS implementation the text may not be cleared when the BIOS is exited. You must also select Start Intel AMT Terminal in order to see the BIOS text displayed. This feature employs user consent, which triggers a 6-digit User Consent code to be displayed on the endpoint's screen. You must contact the endpoint user and enter this code to perform this action.

  **NOTES**

  — If the current emulation does not render correctly, you can choose a different emulation type.

  — If the BIOS rendering is flickering, you can choose a different terminal size.

- **Disconnect** - Disconnects the session.

**NOTE**

If you run Windows PowerShell in the terminal window, do not use upper case letters (Shift+<letter key>) when entering commands as this will cause Windows PowerShell to exit and return to the command prompt. The same is true for Ctrl+<any key>. Enter all commands using only lowercase letters. Most commands are not case-sensitive. Refer the following link for case-sensitivity information: https://devblogs.microsoft.com/scripting/weekend-scripter-unexpected-case-sensitivity-in-powershell/

**NOTE**

That enabling Caps Lock allows you to enter upper case letters without exiting Windows PowerShell.

### 6.3.5 Files Tab

Provides in-band remote file browsing functionality. Beginning with Intel® EMA 1.12.0 file names support Unicode characters. Previous versions of Intel® EMA only support ASCII file names.

This tab will be disabled if any of the following are true:

- The endpoint group policy does not allow this action
- The endpoint is not in-band connected to Intel® EMA
- The logged-in user does not have appropriate access permissions to the endpoint

### 6.3.6 Processes Tab

Provides in-band remote process management functionality. This feature is implemented via Windows Management Instrumentation (WMI). Use it to do the following:

- View a list of running processes.
- Launch a new process on the managed endpoint. You must provide the valid local path to the target executable.
- Terminate processes.

This tab will be disabled if any of the following are true:

- The endpoint group policy does not allow this action
- The endpoint is not in-band connected to Intel® EMA
- The logged-in user does not have appropriate access permissions to the endpoint

### 6.3.7 WMI Tab

Allows you to run a Windows Management Instrumentation (WMI) query or WMI action on the target endpoint.

This tab will be disabled if any of the following are true:

- The endpoint group policy does not allow this action
- The endpoint is not in-band connected to Intel® EMA
- The logged-in user does not have appropriate access permissions to the endpoint

## 6.4 Performing Actions on Endpoints

On the **Managed Endpoints** page, select at least one endpoint and click the **Select an endpoint action** drop-down menu.

Available endpoint actions are described in the following subsections.

### 6.4.1 Wake

Sends a wake request to one or more endpoints via Intel® AMT or Wake-On-LAN.

**NOTE**

Wake-On-LAN is only supported on Intel vPro® platforms.

If only one endpoint is chosen, the action will not be performed if any of the following are true:

- If the endpoint group's policy does not allow this action
- If the logged-in user does not have the appropriate access permissions for this endpoint

### 6.4.2 Set Alarm Clock

This Intel AMT feature allows you to set up to 5 alarm clocks for the endpoint. Alarm clocks wake the endpoint at the specified date and time.

**NOTES**

- To view existing alarms, the user must be in the User Group associated with the target Endpoint Group.
- End Group User and End Group Creator user roles with the HasPowerOperationsAccess permission can view, create, and delete alarms.
- Refer Chapter 1 for more information about user roles.

**To Set An Alarm:**

1. From the Endpoint Details page, select **Actions > Alarm Clock**.
2. On the Alarm Clock dialog, clic**k Add New Alarm**.
3. Enter a name for the alarm.
4. Use the controls under **Wake up this endpoint** at to set the date and time of the alarm.
5. If you want the alarm to repeat in the future, select **Recurring** and then specify the days, hours, and minutes for the recurrence.
6. If you want the alarm to be deleted once it has been executed, select **Delete on Completion**.
7. Click **OK** to set the specified alarm.
8. The new alarm clock's name now appears in the top row of the Alarm Clock dialog.

**To Delete An Alarm**

1. To delete an alarm, select **Actions > Alarm Clock** from the Endpoint Details page.
2. Select the desired alarm from the top row of the Alarm Clock dialog and click **Delete**.

### 6.4.3 Sleep/Hibernate/Power off/Restart

This action can be performed on one or more endpoints.

If the target endpoint is in-band connected, the in-band power operation is performed via the endpoint's operating system. If the target is not in-band connected, but has a complete Intel® AMT configuration record, the associated Intel AMT power action (sleep deep, hibernate, power off soft, power cycle soft, respectively) is performed.

If only one endpoint is chosen, the action will not be performed if any of the following are true:

- If the endpoint group's policy does not allow this action
- If the logged-in user does not have the appropriate access permissions for this endpoint

### 6.4.4 Send Alert

Allows you to send an alert message to one or more endpoints (via in-band connection) in the form of a pop-up window.

To send an alert, enter the message to be displayed and select the duration to display the message, then click Send.

If only one endpoint is chosen, the action will not be performed if any of the following are true:

- If the endpoint group's policy does not allow this action
- If the logged-in user does not have the appropriate access permissions for this endpoint
- If the endpoint is not in-band connected to Intel® EMA

### 6.4.5 Remote File Search

Allows you to perform remote file search for one or more endpoints (via in-band connection). The file search relies on Windows Indexing.

Enter a string to search for and click Search. To download a resulting file, simply click it.

If only one endpoint is chosen, the action will not be performed if any of the following are true:

- If the endpoint group's policy does not allow this action
- If the logged-in user does not have the appropriate access permissions for this endpoint
- If the endpoint is not in-band connected to Intel® EMA

### 6.4.6 Stop Managing an Endpoint

Allows you to remove this target endpoint from Intel® EMA. However, this does not prevent the endpoint from reconnecting and re-registering to Intel® EMA in the future. Also, the system is still provisioned. If the system is provisioned, the endpoint's Admin password and Intel MEBx password will be visible.

**NOTE**

It is strongly recommended that you unprovision Intel AMT on the managed endpoint via the Intel® EMA UI prior to stopping management via this command (refer Intel® AMT On-demand Setup on page 59 for how to unprovision Intel AMT using Intel® EMA). Stopping management without unprovisioning Intel AMT first may result in difficulties re-registering the endpoint in Intel® EMA (endpoint is displayed as being owned by another tool).

This action will be enabled only if BOTH of the following are true:

- A single endpoint is selected
- The logged-in user has the appropriate access permissions for the selected endpoint

### 6.4.7 Provision Intel® AMT

Opens the provisioning information for Intel® AMT. Refer Intel® AMT On-demand Setup on page 59 for details.

This action will be enabled only if ALL of the following are true:

- A single endpoint is selected
- The selected endpoint is Intel AMT capable
- The selected endpoint is in-band connected to Intel® EMA
- The logged-in user has the appropriate access permissions for the selected endpoint

### 6.4.8 View Desktops

Allows you to view (without remote input control) multiple remote in-band KVMs for one or more endpoints.

**NOTE**

User consent for in-band KVM will impact the behavior of this feature. Refer Creating New Endpoint Groups on page 31 for details.

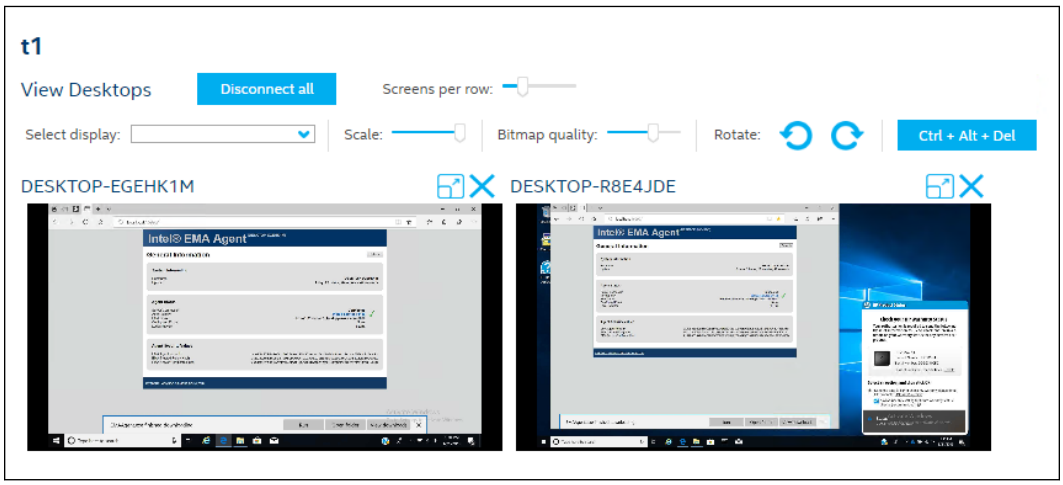
If only one endpoint is chosen, the action will not be performed if any of the following are true:

- If the endpoint group's policy does not allow this action
- If the logged-in user does not have the appropriate access permissions for this endpoint
- If the endpoint is not in-band connected to Intel® EMA

Select the target KVM of an endpoint. Once the target endpoint is highlighted, you can change the display settings and click **Ctrl+Alt+Del** for that target KVM.

You can also click the expand button for each KVM to open the remote KVM tab for that endpoint.

**Figure 9. Multi-desktop Viewing**




## 6.4.9 Mount an Image

Mounts a stored image file (.iso or .img) to the current endpoint via USB Redirection (USBR). For more information on USBR, refer USB Redirection. This menu choice is only available from the endpoint's Details page.

**NOTE**

If the target endpoint's Intel AMT firmware was provisioned in Client Control Mode (CCM) or provisioned in Admin Control Mode (ACM) with the "Consent Required" setting enabled, a 6 digit user consent code is displayed on the endpoint's screen, and you must contact the endpoint user to obtain the code. Once you enter the user's Consent Code, you can then perform this action on the endpoint. Refer Managing Disk Images on page 74 for information about CCM and ACM. Additionally, you can refer to Intel AMT documentation for detailed information about ACM, CCM, and User Consent (https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm).

**To mount an image:**

1. Choose **Mount an Image** from the **Endpoint Actions** drop-down list.Select one of the images from the list.
2. Click **Start**. This triggers a 6-digit User Consent code to be displayed on the endpoint's screen.
3. Contact the endpoint's user and ask for the 6-digit User Consent code which should be displayed on their screen. Enter the code provided.

When the action completes, a **Storage Redirection** banner appears at lower left in the endpoint's Details page, indicating an active USBR session to that endpoint as well as the name of the mounted image file.

To unmount an image file, click **Unmount Image** under the **Storage Redirection** banner on the Details page.

For details on uploading and storing image files, refer Managing Disk Images on page 74.

#### 6.4.9.1 Image Recommendations

Use small images to the greatest extent possible, to prevent timeouts during endpoint reboot to a mounted image. Furthermore, if you plan to interact with the rebooted endpoint via KVM, the image you boot to must contain USB keyboard and mouse drivers.

One recommended method for endpoint reboot to a mounted image is to use a two-part image. First, boot the endpoint to a small image that allows you to bring up the endpoint on your network. Then use that image to access more content from the endpoint.

**NOTE**

There is a current known issue with Intel AMT booting some UDF formatted images via USBR. Sometimes UDF formatted images may not boot or may not boot fully. We recommend using CDFS formatted images until this issue is resolved.

#### 6.4.9.2 Boot to This Image

Reboots the selected endpoint to a mounted image file (.iso or .img).

**NOTE**

You must first mount an image file to the endpoint before performing this action. For more information about mounting image files, Refer Chapter 1.

Once you have mounted an image to this endpoint, click **Boot to this Image** under the **Storage Redirection** banner on the endpoint's Details page.

**NOTE**

It is recommended that you use a signed image file, as Secure Boot in the BIOS will block loading of unsigned images. If Secure Boot blocks the image load, the endpoint may boot to its internal drive.

To verify the endpoint boot operation was successful, use the Hardware Manageability tab and perform a KVM session (Remote Desktop) to the rebooted endpoint to ensure the endpoint booted to the selected image. Images must contain USB keyboard and mouse drivers for KVM interaction.

### 6.4.10 Boot to Recovery Image

Boots the endpoint to the selected recovery image using the Intel AMT One Click Recovery feature.

**CAUTION**

This may erase the endpoint's hard drive. Proceed with caution!

The list of recovery images is populated from preconfigured recovery images on the endpoint platform itself as well as images (i.e., .ISO) that have been uploaded to the Intel® EMA server. However, if for some reason the Recovery Server has been disabled, only the images on the endpoint platform itself will be shown (no uploaded images from the Intel® EMA server).

The images displayed in the list depends on which methods (HTTPS, PBA, or WinRE) are supported on the endpoint platform. If you plan to select an image that uses HTTPS, you must enable HTTPS boot in the endpoint's BIOS. Refer One Click Recovery on page 20 for instructions on this.

**NOTE**

If the target endpoint's Intel AMT firmware was provisioned in Client Control Mode (CCM) or provisioned in Admin Control Mode (ACM) with the "Consent Required" setting enabled, a 6 digit user consent code is displayed on the endpoint's screen, and you must contact the endpoint user to obtain the code. Once you enter the user's Consent Code, you can then perform this action on the endpoint. Refer Intel® AMT Provisioning/Setup Flow in Intel® EMA on page 16 for information about CCM and ACM. Additionally, you can refer to Intel AMT documentation for detailed information about ACM, CCM, and User Consent (https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm).

**To boot to a recovery image:**

1. Select one of the recovery images from the list.
2. Click **Start** and confirm that you want to perform this action. This triggers a 6-digit User Consent code to be displayed on the endpoint's screen.
3. Contact the endpoint's user and ask for the 6-digit User Consent code which should be displayed on their screen. Enter the code provided.

At this point the endpoint reboots to the selected recovery image.

### 6.4.11 Platform Erase

Remotely erases all platform information, including (optionally) the platform's Intel AMT information.

**NOTE**

If the target endpoint's Intel AMT firmware was provisioned in Client Control Mode (CCM) or provisioned in Admin Control Mode (ACM) with the "Consent Required" setting enabled, a 6 digit user consent code is displayed on the endpoint's screen, and you must contact the endpoint user to obtain the code. Once you enter the user's Consent Code, you can then perform this action on the endpoint. Refer Intel® AMT Provisioning/Setup Flow in Intel® EMA on page 16 for information about CCM and ACM. Additionally, you can refer to Intel AMT documentation for detailed information about ACM, CCM, and User Consent (https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm).

After selecting **Platform** Erase from the drop-down menu, select the platform erase options you wish to perform.

| Complete Factory Reset | Selects All Options |
|---|---|
| SSD Erase | Removes all content from ATA and NVM drives through a combination of media erase and crypto erase. |
| Clear BIOS Non-Volatile Memory | Clears the BIOS memory. |
| Reset BIOS Back to Factory State | Resets all BIOS options back to factory defaults. |
| TPM Clear | Resets the Trusted Platform Module (TPM) to its default state, clearing any stored keys. |
| Unconfigure Intel CSME | Unprovisions Intel AMT for remote management.<br>***Caution:*** If you select this option, Intel AMT will be completely unconfigured and you will not be able to perform any Out-of-band (OOB) actions on this endpoint, including mounting a recovery image. However, once Intel AMT has been unconfigured, you can reconfigure Intel AMT on this endpoint using the normal Intel® EMA process like any brand new endpoint. |
| SSD Master Password | Required if **SSD Erase** is selected to **Optional**. |

After selecting desired options, click **Start Erase**. Confirm that you want to perform this action.

# 7.0 Managing Disk Images

**Roles**: Tenant Administrator

Intel® EMA allows you to upload and store bootable disk image files (*.iso and *.img). You can define the default image file storage location by editing the Manageability Server setting **USBR Images Root Directory**. Refer Appendix - Modifying Component Server Settings on page 81 for information on updating component server settings (this setting is under Manageability Server).

**NOTE**

Intel® EMA's automated cleanup processes will periodically remove any folders and files in the USBR root directory that were not created by Intel® EMA. You can also run this cleanup procedure **fileuploadcleanup** manually (see Performing Basic Controls on Component Servers under Using the Intel® EMA Platform Manager Client Application in the Intel® EMA Server Installation and Maintenance Guide or the Intel® EMA Distributed Server Installation and Maintenance Guide

For more information on the USBR feature, refer USB Redirection.

## 7.1 Uploading Image Files

Follow the steps below to upload a disk image file.

1. Select **Storage** from the navigation bar at left, then click the **Disk Images** tab.
2. Click the **Upload** button.
3. In the **Upload Image File** dialog, optionally enter a **Description**.
4. If recovery is from HTTPS and the BIOS allows Intel AMT to control this setting and Intel AMT was provisioned in ACM mode, do NOT select **Enforce Secure Boot**. Otherwise select it.
5. Click **Choose File**.
6. Browse to the desired file, select it, and click **Open**. The dialog displays the file size and the available disk space in the default image file storage location. Refer Appendix - Modifying Component Server Settings on page 81 for information on updating the setting USBR Images Root Directory (under Manageability Server)

   **NOTES**

   - If the selected file's size exceeds the available disk space, an error message is displayed and the Upload button is disabled. Refer Appendix - Modifying Component Server Settings on page 81 for information on setting maximum storage capacity limits for each tenant as well as for the Intel® EMA instance as a whole (under Manageability Server).
   - It is strongly recommended that you do not upload confidential data.

7. Click **Upload**. A progress bar is displayed. To cancel the upload, click **Cancel** (you will be prompted to confirm the cancellation).
8. When the file upload completes, click **Done**. The uploaded file now appears in the list of stored files.

## 7.2 Editing and Deleting Stored Image Files

You can edit and delete image files that you have uploaded. Follow the steps below.

1. Select **Storage** from the navigation bar at left, then click the **Disk Images** tab.
2. In the list of files on the **Storage** page, click the down-arrow in the row of the file you want to edit or delete, then select either **Edit** or **Delete** from the drop-down menu. If you select **Delete**, you are prompted to confirm this choice. If you select **Edit**, a dialog box is displayed. Image files in use cannot be deleted or renamed.
3. In the editor dialog box, edit the file name and/or **Description** as desired.

   **NOTE**

   For file name, only extensions .img and .iso are accepted.

4. Click **Save** to save changes and return to the **Storage** page.

## 7.3 Viewing and Managing Active Sessions

To view and manage active sessions for the current tenant, select **Storage** from the navigation bar at left, then click **Active Sessions** tab.

The active sessions list displays the following information:

| | |
|---|---|
| **Endpoint Name** | Name of the endpoint. |
| **File name** | The image file currently mounted to the endpoint via storage redirection. |
| **Idle Time** | Length of time the session has been idle. |
| **Session Length** | Total length of time since the session was initiated. |
| **User** | User that initiated the session. |
| **End Session** | Click the link to disconnect the session for this endpoint. |

To disconnect an active redirection session, click **End session** in the table row of the target endpoint. You will be asked to confirm this action.

## 7.4 Image Recommendations

Use small images to the greatest extent possible, to prevent timeouts during endpoint reboot to a mounted image. Furthermore, if you plan to interact with the rebooted endpoint via KVM, the image you boot to must contain USB keyboard and mouse drivers.

One recommended method for endpoint reboot to a mounted image is to use a two-part image. First, boot the endpoint to a small image that allows you to bring up the endpoint on your network. Then use that image to access more content from the endpoint.

**NOTE**

There is a current known issue with Intel AMT booting some UDF formatted images via USBR. Sometimes UDF formatted images may not boot or may not boot fully. We recommend using CDFS formatted images until this issue is resolved.

# 8.0 Appendix: Troubleshooting

| Issue | Description |
|---|---|
| Cannot log in to Intel® EMA website | The Intel® EMA website user interface (UI) uses cookies. If you disable cookies in your browser, the Intel® EMA website UI will not work. |
| Intel® EMA Agent Cannot Connect to Intel® EMA Server | Refer Verifying and Troubleshooting Agent Installation on page 51 for information on troubleshooting the Intel® EMA Agent. |
| Endpoint list web page not showing any endpoint or slow to load | If you cannot see any endpoint on the endpoint list web page, do the following:<br>1. Make sure that you understand Section 1.2 and your current logged-in user account has the correct access right to see the target endpoints.<br>2. Make sure that the correct endpoint policy file is used when the Intel® EMA Agent is installed on the target endpoint.<br>3. If you are using Microsoft Enterprise Mode Schema 2 for Internet Explorer and/or Edge, you may need to remove the DNS entry of the Intel® EMA server from the Sites.xml file.<br>4. If all of above are fine, please follow the procedure in **Intel® EMA Agent Cannot Connect to Intel® EMA Server** above. |
| KVM shows a black screen | When connected to Intel AMT KVM, a black screen is displayed if no physical monitor is plugged in.<br>If the endpoint is headless, the Graphics Processing Unit (GPU) powers down if no requests are coming via the operating system. In this case, when the endpoint is power cycled or booted to the BIOS, it detects no attached monitor and powers down the GPU, which results in a black/blank screen. |
| Intel® EMA Agent – Failure during Uninstall or Update | To uninstall the service, or to install/update the service on top of an existing installation, you need to use an Intel® EMA Agent installer with the same architecture type (32-bit service or 64-bit service) as the existing Intel® EMA Agent. |
| Intel® EMA Agent logs | The Intel® EMA Agent generates the following logs:<br>• a general log for errors encountered when the Agent is running<br>• a debugging log for debug information<br>• an installation log if any errors are detected during the install/uninstall process<br>**General Intel® EMA Agent error log**<br>The general log is enabled by default, and it reports Intel® EMA Agent service errors. The file name is **EmaAgent.log**.<br>The **EmaAgent.log** file is located in the Intel® EMA Agent installation directory in the **Program Files** folder for win64.<br>Logs include the date and time of the error, the path and file name of the error, line numbers, parameters, and a brief description of the error.<br>Log file syntax:<br>`[Date & Time] FilePath: LineNumber (Parameter1, Parameter2) Message.`<br>**Intel® EMA Agent installation log** |

***continued...***

| Issue | Description |
|---|---|
| | This log is generated when an error is detected during the install/uninstall process. The log file is named after the installer used, and is located in the same folder where the installer is located. If no errors are detected during the install/uninstall process, the log is not created.<br>*Note:* To address the specific error message "Error removing the installation directory file," ensure there are no open or protected files in the installation directory when uninstalling. Be sure to close all files before starting the uninstall. |
| Intel® EMA states the endpoint is managed by something else | The endpoint may be managed currently by another management application. To allow Intel® EMA to manage it, you need to unprovision the endpoint and then reprovision it using Intel® EMA. Refer your Intel AMT documentation (below) for information on unprovisioning.<br>https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm<br>Alternatively if the Intel AMT Admin password is known, you can use the POST /api/latest/amtSetups/endpoints/adopt API to adopt the endpoint.<br>Refer the swagger documentation for more information. |
| Importing PKI certificate fails on Windows Server 2016 | If you have installed the Intel® EMA Server on a machine running Windows Server 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.<br>This is a Windows issue in which Windows itself does not support PFX files created using this encryption. This issue is fixed starting with Windows Server 2016 build 1709 and later.<br>https://github.com/dsccommunity/CertificateDsc/pull/154/files<br>**To fix:**<br>1. Install the PFX file on a system that supports the PFX file with encryption "AES256-SHA256" (for example, Windows 10 desktop). To do this, double click the PFX file to launch the Certificate Import Wizard. By default it will install to the currently logged-in user's personal certificate store. Be sure to select **Mark this key as exportable** and **Include all extended properties.**<br>2. Open Microsoft Management Console for current user certificates.<br>3. Right-click on the certificate that was just installed, then select **All Tasks> Export....** This will open the Certificate Export Wizard.<br>4. In the wizard, select **Yes, export the private key** and click **Next**.<br>5. Select **Personal Information Exchange (.PFX)** and select **Include all certificates in path**, **Export all extended properties**, and **Enable certificate privacy**. If desired, select **Delete the private key if successful** (do this if you want to remove the certificate and key from this intermediate system). Click **Next**.<br>6. On the security screen select the **Encryption** "TripleDES-SHA1". This is basis of the issue: older versions of Windows do not support PFX files with "AES256-SHA256". This encryption is not for the actual certificate , but rather it is used along with the password provided on this screen to protect the private key associated with the certificate when it is exported out to the PFX file format.<br>7. Finish the export wizard screens to create a new PFX file. This new PFX file can be successfully used on the older Windows system on which you installed the Intel® EMA server. |

***continued...***

| Issue | Description |
|---|---|
| In-band KVM paste from clipboard results in unexpected characters or case | When attempting to paste plain text from the clipboard of the Intel® EMA console system (i.e., the clipboard of the computer running the Intel® EMA web-based UI) to an endpoint via KVM, you may notice unexpected case or capitalization in the pasted output on the target endpoint. This is consistent with other remote desktop applications' behavior. For more information, refer the following link from Microsoft:<br>https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/caps-lock-key-status-not-synced-to-client<br>Further, depending on the OS language/locale of the target endpoint, unexpected characters may be pasted. Only US English keyboard character codes are supported. If the endpoint's language/locale is not US English, unpredictable characters may be pasted on the endpoint.<br>**To fix (capitalization issue only):**<br>Ensure that the Caps Lock is OFF on the target endpoint before pasting. If you pressed Caps Locks during a KVM session to that endpoint, be sure to press Caps Lock again before exiting the KVM session to clear (turn off) the Caps Lock on the target. Otherwise Caps Lock will remain ON on the endpoint, and when you paste to that endpoint, the pasted text will behave accordingly (lower case as all caps, and vice versa). |
| Exporting PFX using Server Certificates API fails | Periodically, calling the POST /api/latest/serverCertificates/{certificateName}/getPFX will result in an error. If this occurs, wait for a minute and then retry the call again. |
| Provisioning errors on devices ME19+, examples:<br>• Error with cert chain : (<device_name>) | Make sure the Intel "OnDie CA Root Cert Signing" (subject "www.intel.com") certificate is installed in your Intel® EMA server local computer cert store (Intel® EMA installs this by default) |
| Endpoint with ME20+ is stuck in "pending configuration" state when using 802.1x and client certificate is generated by a CA. | AMT cert template could be configured to use RSA 2048: ME20+ will use ECDH 384 (highest available), you will need to create a template to use the proper crypto lib and change your 802.1x profile in Intel® EMA to point to the new template. |
| The failure from the EMA logs is **"Warning(s) - Error with CRL check of Level1 cert..."** | Make sure the server where Intel® EMA is installed has internet access. If this is not possible, continue with the next step. Disable CRL checking, this configuration is in the Intel EMA web application:<br>1. Log into the EMA web console with a Global Admin account<br>2. Go to Settings -> Manageability Server<br>3. Scroll down to the "Enable Provisioning TLS Certificate Revocation Check" option. **Uncheck this option.** (This should be **disabled**)<br>4. Scroll up, and click on "Save and Restart Server" button near top<br>5. Reboot the EMA server |
| SAML Authentication Errors | If users cannot authenticate, check that the user exists in the IDP and it doesn't contain typos in any SAML Entity ID (case sensitive) and MetaURL,<br>For specific debug information, check the EMA web server logs. Under C:\Program Files (x86)\Intel\Platform Manager\EMALogs\EMALog-WebServer.txt |
| Having trouble Users for SAML authentication | EMA accepts email-like formatted usernames, meaning that only claims with that format will we valid<br>The SAML application in the IDP must be configured to include a claim containing the user's UPN in a valid email format. Our system will use the first available non-empty value in email format from the following claims, in this order: nameidentifier, upn, emailaddress and name.<br>List the priority of the claim checks (metadata file): |

***continued...***

| Issue | Description |
|---|---|
| | http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier<br>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn<br>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress<br>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name |
| Intel® EMA Website Fails to Load Due to Web.config and ApplicationHost.config Conflicts - Duplicate Trace Verb entry | Intel® EMA may fail to load due to conflicting configuration values between Web.config and ApplicationHost.config files. You can detect this issue by opening IIS Manager and checking the specific settings that show configuration conflicts.<br>Starting with EMA version 1.14.x, a new HTTP TRACE verb was introduced, which can cause configuration conflicts. To resolve this issue:<br>Open the EMA IIS Web.Config, locate and remove this key <add verb="TRACE" allowed="false" /> |
| Running Intel® EMA Agent in console mode, the KVM session may display only a blank screen if the agent lacks proper administrative privileges. | Running Intel® EMA Agent in console mode, the KVM session may display only a blank screen if the agent lacks proper administrative privileges.<br>To resolve this issue, ensure the Intel® EMA Agent is launched with administrator privileges using one of these methods:<br>1. Right-click method: Right-click the EMA Agent executable and select "Run as administrator"<br>2. Command line method: Open Command Prompt as administrator and launch the agent from the command line.<br>Running the agent without administrator privileges will prevent the KVM session from displaying properly, resulting in a blank screen during remote console access. |

# 9.0 Appendix - Modifying Component Server Settings

The settings for the various component servers (Swarm Server, Ajax Server, etc.) that comprise the Intel® EMA server can be modified using the **Server Settings** tab, which is accessible from the **Settings** selection on the vertical navigation pane at left. To modify security settings for the component servers, select the **Security Settings** tab. Refer Security Settings for a list of security settings and descriptions.

The following subsections describe the settings available for each of the component servers. For each component server, settings are listed in the order they appear in the Intel® EMA user interface pages.

**NOTE**

If you change the **serverIps** or **messagePort** setting for any of the component servers, you must restart all the component servers, not just the one whose settings you changed (in a distributed server architecture, you must do this on all server machines). Also, you will need to recycle the Intel® EMA web site's IIS application pool to restart the Intel® EMA web server when you change these two settings. For other settings, restarting only the modified component server will suffice. If you change **messagePort**, make sure the new port is not blocked by a firewall.

## 9.1 Swarm Server

| Setting | Description |
|---|---|
| **UI: Admin Port**<br>**API: adminport** | The port that Swarm Server's Admin TCP listener will bind to. This is for communication from other Intel® EMA server processes to the Swarm server. The default is 8089. |
| **UI: Admin Port Local**<br>**API: adminportlocal** | Determines if the Admin TCP listener will only bind to the local loopback or not. Values are 0 and 1.<br>0 = Distributed-server environment<br>1 = Single server environment |
| **UI: Agent Auto Update**<br>**API: enableAgentAutoUpdate** | Boolean. Enables or disables automatic agent update. Default: Enabled. |
| **UI: Agent Update Interval (Seconds)**<br>**API: agentUpdateIntervalSeconds** | Interval in seconds between Intel® EMA Agent updates. I.e., if set to 5, the Intel® EMA server will wait 5 seconds before attempting to update the next agent requesting update.<br>Default: 10.<br>Minimum: 10.<br>Maximum: 120. |
| **UI: Log File Path**<br>**API: logfilepath** | Path to the Intel® EMA logfile.<br>Maximum: 247 characters<br>Minimum: 2 characters |
| **UI: Enable Intel CIRA Power State Polling**<br>**API: enableCIRAPowerPolling** | Enable periodic CIRA power state polling. Values are True/False. The default is True. |

***continued...***

| Setting | Description |
|---|---|
| **UI: Maximum Number of Concurrent Database Connections**<br>**API: maxdbconnections** | The maximum number of concurrent DB connections for this server. |
| **UI: Swarm Servers**<br>**API: swarmserver** | List of active Swarm Servers. Includes Server ID and Server IP & Port (format IP Address: port). |
| **UI: Server Ips**<br>**API: serverIps** | List of machine IP addresses where this component server type is running. For example, if the Swarm server is running on machine ip1, ip2, and ip3, then serverIps will include all IP addresses. |
| **UI: Message Port**<br>**API: messagePort** | The TCP port this component server type is listening on to accept internal traffic from other Intel® EMA components. Default 8093. |
| **UI: TCP Connection Retry**<br>**API: tcpConnRetrySeconds** | Wait time between retries when establishing communication connections between Intel® EMA server components. |
| **UI: TCP Connection Idle**<br>**API: tcpConnIdleSeconds** | Interval between heartbeat messages sent between components once communications are established. |
| **UI: Database Connection Wait Time (Minutes)**<br>**API: dbConnectionWaitTimeMinutes** | Amount of time in minutes that Intel® EMA will wait for getting a database connection.<br>Range: 1 - 10<br>Default: 2 |
| **UI: Database Lock Timeout Period (Seconds)**<br>**API: dbSetLockTimeoutSeconds** | Amount of time in seconds that a SQL query will keep a lock.<br>Range: 1 - 60<br>Default: 2 |
| **UI: Database Retry Hold Time for a Query (Milliseconds)**<br>**API: dbRetryHoldtimeMilliSeconds** | Amount of time in milliseconds that a SQL query will wait to complete. This value is multiplied by the value of Database Retry Attempts for a Query to increase the hold time in each retry.<br>Range: 100 - 60000<br>Default: 100 |
| **UI: Database Retry Attempts for a Query**<br>**API: dbRetryMaxAttempts** | Number of retries to execute a failed SQL query. After reaching this value, the Swarm server will restart due to critical failure in the database.<br>Range: 3 - 100<br>Default: 5 |
| **UI: CIRA Keep-alive Interval (Seconds)**<br>**API: CIRAKeepAliveIntervalSeconds** | Sets the interval, in seconds, for the Swarm Server's periodic messages to the target endpoint's Intel AMT firmware to keep the CIRA connection open. New installations of Intel® EMA will have a default value of 10 minutes. Upgrading from an older version of Intel® EMA, prior to 1.11.0, will have a default value of 10 seconds.<br>Default: 10 seconds<br>Min: 10 seconds<br>Max: 1 hour (i.e., 3,600 seconds) |

## 9.2 Ajax Server

| Setting | Description |
|---|---|
| **UI: Ajax Cookie Auto Refresh Range**<br>**API: ajaxCookieAutoRefreshRange** | Range in minutes in which the Ajax cookie life can be extended. |
| **UI: Ajax Cookie Idle Timeout**<br>**API: ajaxCookieIdleTimeout** | Amount of time, in minutes, from when the cookie is added until it expires. |

*continued...*

| Setting | Description |
|---|---|
| **UI: Http Header Access Control Allow Headers**<br>**API: httpheader_Access-Control-Allow-Headers** | Additional headers to set in response to the Ajax request. |
| **UI: Log File Path**<br>**API: logfilepath** | Path to the Intel® EMA logfile.<br>Maximum: 247 characters<br>Minimum: 2 characters |
| **UI: User Access Failed Max Count**<br>**API: userAccessFailedMaxCount** | Number of failed password attempts before user account is locked by the Web API. |
| **UI: Expire Sessions**<br>**API: expiresessions** | Sets whether the Ajax server should expire the session or not (default is enabled). |
| **UI: Maximum Number of Concurrent Database Connections**<br>**API: maxdbconnections** | The maximum number of concurrent DB connections for this server. |
| **UI: Server IPs**<br>**API: serverIps** | List of machine IP addresses where this component server type is running. For example, if the Ajax server is running on machine ip1, ip2, and ip3, then serverIps will include all IP addresses. |
| **UI: Swarm Servers**<br>**API: swarmserver** | List of active Swarm Servers. Includes Server ID and Server IP & Port (format IP Address: port). |
| **UI: Message Port**<br>**API: messagePort** | The TCP port this component server type is listening on to accept internal traffic from other Intel® EMA components.<br>Default 8092. |

## 9.3 Manageability Server

| Setting | Description |
|---|---|
| **UI: CIRA Server Host**<br>**API: ciraserver_host** | Hostname of the CIRA access server, which is the Swarm Server (or the Swarm Server load balancer in a distributed architecture). Only used when the installation mode is using hostname. This is used in multi-server installations. |
| **UI: CIRA Server IP**<br>**API: ciraserver_ip** | IP Address of the CIRA access server, which is the Swarm Server (or the Swarm Server load balancer in a distributed architecture). Only used when the installation mode is using IP address. |
| **UI: Log File Path**<br>**API: logfilepath** | Path to the Intel® EMA logfile.<br>Maximum: 247 characters<br>Minimum: 2 characters |
| **UI: Maximum Number of Concurrent Database Connections**<br>**API: maxdbconnections** | The maximum number of concurrent database connections for this server. |
| **UI: USBR Images Root Directory**<br>**API: usbrImagesRootDirectory** | The root directory on the Intel® EMA server where uploaded bootable image files (.iso and .img) are stored. Default value is **C:\ProgramData\Intel\EMA\USBR**.<br>*Note:* If this folder is changed by the Global Administrator after images have been uploaded, the files will not be visible or available to other users like the Tenant Administrator. The Global Administrator (system administrator) will need to manually copy the content from the original folder to the new folder before other users can access the files. |

***continued...***

| Setting | Description |
|---|---|
| **UI: Maximum USBR Image Storage Capacity per Tenant**<br>**API: maxUsbrImageStorageCapacityPerTenantInGigabytes** | Disk space in GB each tenant is allowed for USBR image storage.<br>Default: 20 GB<br>Maximum: 50 GB |
| **UI: Maximum USBR Image storage Capacity Per EMA Instance**<br>**API: maxUsbrImageStorageCapacityPerEmaInstanceInGigabytes** | Total disk space in GB (for all tenants) allowed in this Intel® EMA instance for USBR image storage.<br>Default: 50 GB<br>Maximum: 500 GB |
| **UI: Maximum USBR Slot Count per Tenant**<br>**API: maxUsbrSlotCountPerTenant** | Number of active USBR sessions allowed for each tenant. |
| **UI: Maximum USBR Idle time**<br>**API: maxUsbrIdleTimeInMinutes** | Length of time in minutes a USBR session can be idle before being automatically terminated. |
| **UI: USBR Redirection Manager Loop Interval**<br>**API: usbrRedirectionManagerLoopIntervalInSeconds** | Status polling interval in seconds for active USBR sessions. |
| **UI: USBR Redirection Throttling Rate**<br>**API: usbrRedirectionThrottlingRateInMilliseconds** | The delay in sending USBR file data to the target endpoint's Intel AMT firmware. This is needed in order to throttle the data rate, as certain internal data flows within Intel® EMA do not work properly if the data rate is too high.<br>*Note:* CIRA based provisioning is highly recommended when using USBR. USBR is sensitive to latency and Intel® EMA has optimized USBR for CIRA provisioned endpoints. If you are using TLS with relay, you will need to adjust the "USBR Redirection Throttling Rate" under the Manageability Server section in Server Settings as a Global Admin. This setting is dependent upon your unique network environment. We recommend starting at a setting of 10 milliseconds and increasing it in increments of 10 until you find a rate that works well in your network environment. It is unlikely you would need to go above of 50 milliseconds. Note that increasing this setting will decrease the USBR boot performance, especially for CIRA endpoints, and should only be used for TLS with relay only instances.<br>Default value: 0, max value 1000, min value 0.<br>Suggested value = start at 10, increment by 10 to find appropriate rate for your network. |
| **UI: File Upload Retention Period**<br>**API: fileUploadRetentionPeriodInDays** | Number of days an incomplete resumable file upload would be kept, after which it would be automatically deleted. |
| **UI: File Upload Cleanup Interval**<br>**API: fileUploadCleanupIntervalInHours** | Interval in hours that file cleanup process would run to process incomplete resumable files. |
| **UI: Swarm Servers**<br>**API: swarmserver** | List of active Swarm Servers. Includes Server ID and Server IP & Port (format IP Address: port). |
| **UI: Server IPs**<br>**API: serverIps** | List of machine IP addresses where this component server type is running. For example, if the Manageability server is running on machine ip1, ip2, and ip3, then serverIps will include all IP addresses |

*continued...*

| Setting | Description |
|---|---|
| **UI: Message Port**<br>**API: messagePort** | The TCP port this component server type is listening on to accept internal traffic from other Intel® EMA components. Default 8094. |
| **UI: Audit Log Cleanup Interval (Hours)**<br>**API: AuditLogCleanupIntervalInHours** | Interval in hours before cleanup of audit log records in the Intel® EMA database. |
| **UI: Audit Log Retention Period (Days)**<br>**API: AuditLogRetentionPeriodInDays** | Interval in days before cleanup of audit log records in the Intel® EMA database. |
| **UI: Enable 8021X Certificate Auto Renewal**<br>**API: Is8021XCertificateRenewalEnabled** | Boolean, default "True." Used to determine whether automatic 802.1x certificate renewal flows are enabled. If enabled, Intel® EMA automatically renews certificates that will be expiring soon. |
| **UI: 802.1X Certificate Renewal Window (Days)**<br>**API: Ieee8021xCertificateRenewalWindowDays** | Integer. Sets the number of days prior to an 802.1x certificate's expiration at which Intel® EMA flags that certificate for renewal.<br>Default: 30<br>Maximum: 90<br>Minimum: 1 |
| **UI: Enable Provisioning TLS Certificate Revocation Check**<br>**API: enableProvisioningTLSCertCRLCheck** | Boolean. Enables or disables Certificate Revocation List (CRL) checking for the provisioning TLS certificate provided by the client Intel AMT systems in TLS provisioning flows. CRL checking requires the Manageability Server to have an active internet connection for periodic downloads of the CRL files.<br>Default: True. |

## 9.4 Web Server

**NOTE**

Use the **Save and Sync Web Settings** button to restart the web server. Alternatively, you can run the Intel® EMA installer EMAServerInstaller.exe (as Administrator) and select **Settings > Sync Web Server Settings** from the menu bar.

| Settings | Description |
|---|---|
| **UI: Access Token Time to Live**<br>**API: AccessTokenTimeToLive** | Expiration duration of the API bearer token, in seconds. |
| **UI: Ajax Server Host**<br>**API: AjaxServerHost** | Hostname or IP address of the Ajax server, or the load balancer of the Ajax servers. |
| **UI: Enable Allowed Domains, Allowed Domains**<br>**API: EnableAllowedDomains, AllowedDomains** | Used by the Ajax server. If enabled, the web server checks incoming Ajax/websocket requests to accept or reject.<br>AllowedDomains is a comma delimited list with example test1.intel.com,test2.intel.com.<br>EnableAllowedDomains is 0 (false) or 1 (true). |
| **UI: Log File Path**<br>**API: logfilepath** | Path to the Intel® EMA logfile.<br>Maximum: 247 characters<br>Minimum: 2 characters |
| **UI: Maximum Number of Concurrent Database Connections**<br>**API: maxdbconnections** | The maximum number of concurrent database connections for this server. |

***continued...***

| Settings | Description |
|---|---|
| **UI: Swarm Server Host**<br>**API: SwarmServerHost** | Hostname or IP address of the Swarm server, or the load balancer of the Swarm servers. |
| **UI: Swarm Server LegacyPort**<br>**API: SwarmServerLegacyPort** | 8080 in single server installation or the Swarm server port exposed by the swarm server load balancer in distributed server architecture. Uses 2048-bit keys. |
| **UI: Swarm Server Port**<br>**API: SwarmServerPort** | 8081 in single server installation or the Swarm server port exposed by the swarm server load balancer in distributed server architecture. Uses 3072-bit keys. |
| **UI: Global Catalog Port**<br>**API: GlobalCatalogPort** | The port used for connecting to the Active Directory Global Catalog. This is used to perform AD login when AD username and password are provided. Default is 3269, which is the SSL port.<br>Refer the note for LDAP Connection Port below. |
| **UI: LDAP Connection Port**<br>**API: LdapConnectionPort** | The port used for LDAP connection in 802.1x configuration. Default port is secure 636.<br>*Note:* Intel® EMA version 1.5.0 and later uses LDAPS secure ports by default (LDAPS secure port 636 and Global Catalog port 3269). Previous versions of Intel® EMA used the standard non-secure LDAP ports (LDAP port 389 and Global Catalog port 3268). If you are installing Intel® EMA v 1.5.0 or later, and are using Active Directory or 802.1x integration, ensure the LDAPS ports are enabled. If you prefer to use the standard non-secure ports, then after installing Intel® EMA, open the installer program again (EMAServerInstaller.exe, run as administrator) and select **File > Advanced Mode, then click Settings > Switch from LDAPs to LDAP** to reset the LDAP ports Intel® EMA uses to the standard non-secure ports. Alternatively, you can change the ports in the Web server settings on the Server Settings page in the Intel® EMA UI. If you experience problems with 802.1x setup during Intel AMT provisioning, this could be the issue. Refer the following link for more information: https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts. |
| **UI: Max Access Token TTL**<br>**API: MaxAccesstokenTTL** | Maximum time for API bearer tokens to be refreshed. |
| **UI: Frontend Storage Type**<br>**API: frontendstoragetype** | Allows you to specify whether Intel® EMA Website runtime information should be stored in browser local storage or browser session storage. If Local Storage is used, the session will remain (no need to login again) after the front end website is closed. If Session Storage is used, the session is lost when the front end website is closed. |
| **UI: Azure AD Directory (tenant) ID**<br>**API: AzureAdTenantId** | The Azure AD Directory (tenant) ID in GUID format. Only used when Azure AD authentication option is selected. |

***continued...***

| Settings | Description |
|---|---|
| **UI: Azure AD Application (client) ID**<br>**API: AzureAdClientID** | The Azure AD Application (client) ID in GUID format. Used with the Azure Secret to enable the Web Server to connect to the specified Azure Tenant. Only used when Azure AD authentication option is selected. |
| **UI: Azure AD Client Secret Value**<br>**API: AzureAdClientSecretValue** | The Azure AD Client Secret Value, only used when Azure AD authentication option is selected. Secret will be stored in an encrypted format in the SQL Database. |
| **UI: SAML IDP Entity ID**<br><br>**API: SamlIdpEntityId** | The SAML IDP Entity ID Value, only used when SAML authentication option is selected.<br>Unique identifier for the Identity Provider (IdP) in a SAML authentication setup. It serves as a key component in the SAML metadata, helping to distinguish the IdP from other entities in the SAML ecosystem<br>Entity ID is case-sensitive<br>*Note:* When changing this setting you need to recycle the IIS Appool, reset the website or webserver running the EMA WebSite. |
| **UI: SAML IDP Metadata URL**<br><br>**API: SamlIdpMetadataUrl** | It is a URL provided by the Identity Provider (IdP) that hosts the metadata necessary for establishing trust and communication between the IdP and the Service Provider (SP)<br>Obtain the App Federation Metadata URL from your IdP.<br>Import this metadata into your application's SAML configuration settings.<br>The EMA sever will try to connect to the provided URL to check its validity, make sure the URL reachable before changing this setting.<br>Only HTTP and HTTPS schemes are supported.<br>*Note:* When changing this setting you need to recycle the IIS Appool, reset the website or webserver running the EMA WebSite. |

## 9.5 Security Settings

Most of the security settings below apply across the component servers, although some apply only to a specific component server (for example, the Ajax server). Many of these settings are intended to help prevent Denial of Service (DoS) attacks.

**NOTE**

If you change security settings for any of the component servers, you must restart all the component servers, not just the one whose settings you changed (in a distributed server architecture, you must do this on all server machines). Also, you will need to recycle the Intel® EMA web site's IIS application pool to restart the Intel® EMA web server when you change these settings.

| Settings | Description |
|---|---|
| UI: Unauthorized TCP connection timeout | Boolean. When enabled Intel® EMA will terminate new TCP connections that go idle and do not complete the SSL handshake to help prevent Denial of Service attacks.<br>Default: true. |

***continued...***

| Settings | Description |
|---|---|
| API: enableUnauthTcpConnectionIdleTimeout | |
| UI: TCP connection timeout<br>API: unauthTcpConnectionIdleTimeoutInMilliSeconds | The amount of time in milliseconds a new TCP TLS connection has to complete SSL handshake before the connection is considered idle and terminated.<br>Default: 10000<br>Maximum: 3,600,000 (1 hour) |
| UI: Rate Limiter<br>API: enableRateLimiter | Boolean. When enabled Intel® EMA will perform per-IP address HTTPS/TCP TLS request rate limiting to help prevent Denial of Service attacks.<br>Default: true. |
| UI: Rate Limiter Window Size<br>API: rateLimiterWinSizeInMilliSeconds | The window size in milliseconds to use for tracking requests with per-IP address rate limiting.<br>Default: 200<br>Maximum: 3,600,000 (1 hour) |
| UI: Ajax HTTP Requests Max Count<br>API: ajaxHttpRateLimiterMaxCount | The maximum number of allowed requests per-IP address in a window before requests would be rejected to the Ajax Server Web redirection port (8084).<br>Default: 20<br>Maximum: 1,000,000 |
| UI: Recovery HTTP Requests Max Count<br>API: recoveryHttpRateLimiterMaxCount | The maximum number of allowed requests per-IP address in a window before requests would be rejected to the Recovery Server Web redirection port (8085).<br>Default: 20<br>Maximum: 1,000,000 |
| UI: Message Ports Requests Max Count (Before Authorization)<br>API: blastMessageBeforeAuthRateLimiterMaxCount | The maximum number of allowed pre-authentication requests per-IP address in a window before requests would be rejected to the internal component-to-component ports (8092, 8093, 8094).<br>Default: 100<br>Maximum: 1,000,000 |
| UI: Message Ports Requests Max Count (After Authorization)<br>API: blastMessageAfterAuthRateLimiterMaxCount | The maximum number of allowed post-authentication requests per-IP address in a window before requests would be rejected to the internal component-to-component ports (8092, 8093, 8094).<br>Default: 80,000<br>Maximum: 1,000,000 |
| UI: Swarm Admin Ports Request Max Count (Before Authorization)<br>API: adminPortBeforeAuthRateLimiterMaxCount | The maximum number of allowed pre-authentication requests per-IP address in a window before requests would be rejected to the Swarm Server Admin port (8089).<br>Default: 20,000<br>Maximum: 1,000,000 |
| UI: Swarm Admin Ports Request Max Count (After Authorization)<br>API: adminPortAfterAuthRateLimiterMaxCount | The maximum number of allowed authenticated requests per-IP address in a window before requests would be throttled to the Swarm Server Admin port (8089).<br>Default: 20,000<br>Maximum: 1,000,000 |
| UI: Agent Port Request Max Count (Before Authorization)<br>API: agentPortBeforeAuthRateLimiterMaxCount | The maximum number of allowed pre-authentication requests per-IP address in a window before requests would be rejected to the Swarm Server Agent port (8080, 8081).<br>Default: 20<br>Maximum: 1,000,000 |

*continued...*

| Settings | Description |
|---|---|
| UI: Agent Port Request Max Count (After Authorization)<br>API: agentPortAfterAuthRateLimiterMax Count | The maximum number of allowed authenticated requests per-IP in a window before requests would be throttled to the Swarm Server Agent port (8080, 8081).<br>Default: 1000<br>Maximum: 1,000,000 |
| UI: Connection Count Check<br>API: enableConnectionCountChecker | Boolean. When enabled Intel® EMA will limit the TCP TLS connection count per-IP address to help prevent Denial of Service attacks.<br>Default: true. |
| UI: Message Port (connections per port)<br>API: blastMessageConnCountChecker | The maximum number of connections per-IP address allowed to the internal component-to-component ports (8092, 8093, 8094).<br>Default: 20<br>Maximum: 1,000,000 |
| UI: Admin Port (connections per port)<br>API: swarmAdminPortConnCountCheck er | The maximum number of connections per-IP address allowed to the Swarm Server Admin port (8089).<br>Default: 20,000<br>Maximum: 1,000,000 |
| UI: Swarm Agent Port (connections per port)<br>API: swarmAgentPortConnCountChecker | The maximum number of connections per-IP address allowed to the Swarm Server Agent port (8080, 8081)<br>.<br>Default: 20,000<br>Maximum: 1,000,000 |
| UI: User password minimum length<br>API: userPasswordMinLength | Used to customize policy for password validation.<br>Default: 8<br>Minimum: 8<br>Maximum: 20 |
| UI: User password maximum length<br>API: userPasswordMaxLength | Used to customize policy for password validation.<br>Default: 255<br>Minimum: 64<br>Maximum: 255 |
| UI: Client Credentials minimum length<br>API: clientCredentialsMinLength | Used to customize policy for password validation.<br>Default: 12<br>Minimum: 12<br>Maximum: 20 |
| UI: Client Credentials maximum length<br>API: clientCredentialsMaxLength | Used to customize policy for password validation.<br>Default: 255<br>Minimum: 64<br>Maximum: 255 |
| UI: Complexity required (uppercase/lowercase/special char)<br>API: passwordComplexityRequired | Used to customize policy for password validation.True/False.<br>Default: True |
| UI: Password Disallowed List Checking<br>API: PasswordDisallowedListChecking | Boolean. When it is enabled and user authentication(username/ password) is used, if a new user is created or a current user has password updated, the supplied password will be checked against a disallowed password list. This list can be customized by using the Installer Advanced Mode.<br>Default: True. |
| UI: 2FA TOTP Algorithm<br>API: MfaTotpAlgorithm | Used to indicate the algorithm used by MFA TOTP. 0 means SHA1, 1 means SHA256, and 2 means SHA512.<br>Default: 0<br>Minimum: 0<br>Maximum: 2 |

## 9.6 Recovery Server Settings

The settings below are provided to support future Intel platforms.

| Settings | Description |
|---|---|
| UI: Log File Path<br>API: logfilepath | Path to the Intel® EMA logfile.<br>Maximum: 247 characters<br>Minimum: 2 characters |
| UI: Maximum Number of Concurrent Database Connections<br>API: maxdbconnections | The maximum number of concurrent database connections for this server. |
| UI: Message Port<br>API: messagePort | The TCP port this component server type is listening on to accept internal traffic from other Intel® EMA components. Default 8095. |
| UI: Recovery Port<br>API: RecoveryPort | Port to be used for recovery. Default 8085.<br>*Note:* If you change the default port, you will be prompted to update port bindings by running the following commands in admin mode on each recovery server in this Intel® EMA installation (items in brackets <> are provided in the prompt popup dialog):`netsh http delete sslcert ipport=<original port number>netsh http add sslcert ipport=<new port number>certhash=<certificate hash>appid={3a6739cf-6707-4623-a073-34b6b7a51b1d}` |
| UI: Recovery Port Enabled<br>API: RecoveryPortEnabled | Boolean, default "True." Specifies whether or not the recovery port is enabled. |
| UI: Server IPs<br>API: serverIps | List of machine IP addresses where this component server type is running. For example, if the Ajax server is running on machine ip1, ip2, and ip3, then serverIps will include all IP addresses. |

# 10.0 Appendix - Intel® EMA Agent Console

The Intel® EMA Agent is typically installed and run as a service. However, it can also be run as a console or a standalone executable application. This can be useful if you want to install the Agent on a system where you do not want to run it as a service, but rather run it "on demand" by executing it manually. The functionality is the same as the service version.

The Intel® EMA Agent console is available for download from the Intel® EMA API.

**NOTES**

- The console version of the Agent executable has the same file name (EmaAgent.exe) as the service version. So if you want to download the console agent to a system that has Agent already installed as a service, be sure to rename the console version so that it doesn't overwrite the service Agent.
- The Agent console is a command line tool and does not have a graphical user interface.
- The Agent console can be used for Agent installation troubleshooting, just like the service version. Refer Deploying the Agent to Your Endpoints on page 49 for details.

## 10.1 Files

There are two files you need to install Intel® EMA Agent as a console or a standalone executable application. The properties of these files are described in the table below. These two files must be co-located in the same directory. Be sure to download the agent console application into the correct folder for the architecture of the system you are downloading to (C:\Program Files\Intel\Ema Agent).

| File Name | Description |
|---|---|
| **EmaAgent.exe** | This is the Agent's installation file. You must execute this file with administrative privileges to install/update/uninstall any instance. |
| **EmaAgent.msh** | This is the policy file. This file determines which Endpoint Group the endpoint will belong to and enables the Intel® EMA Agent to contact the Intel® EMA server. |

To run the Intel® EMA Agent as a console, do the following on a managed endpoint system:

1. Open a command window (cmd.exe) with administrative privileges and go to the path where the Intel® EMA Agent console executable is located.
2. Run the following command to start the Intel® EMA Agent in console mode (if you changed the file name, use the name you chose):

   ```
   EmaAgent.exe
   ```

3. To stop the Intel® EMA Agent in console mode use the key combination **CTRL+C**.

## 10.2 Intel® EMA Agent Database

Once the Agent service is installed, a local database is generated to save settings and certificates. The database is stored in the same path as the agent's running executable binary.

## 10.3 Proxy Configuration

To configure a proxy for use in console mode you must add the proxy argument when starting the console. Run the following command:

EmaAgent.exe –proxy:host:port

- Host: HTTPS hostname of the proxy.
- Port: Port number of the proxy

## 10.4 Resource Consumption

Resource consumption is divided per CPU, RAM, and network traffic.

All of the following tests are performed on a DELL laptop, model Latitude E7270, with Windows 10 Professional 64-bit, an Intel® Core™ i5-6300 2.40 GHz – 2.5 GHz processor, and 16GB RAM in a local LAN with wired network.

**CPU**

- The max average without any connection to the Agent's console is 0.01%.
- The max average using a remote desktop is 5.53%.
- The max average using a terminal is 0.29%. This is a result of using the console command and operations such as ipconfig, ipconfig /all, or netstat.
- The max average using the file manager is 3.11%. The uploaded file is 133 MB.

**RAM**

The values in this section are taken from the Working Set (KB) column in Windows Resource Monitor.

- The max average without any connection to the Agent is 33,380 KB.
- The max average using a remote desktop is 51,040 KB.
- The max average using a terminal is 33,632 KB.
  - This is a result of using the console command and operations such as ipconfig, ipconfig /all, or netstat. This average may increase significantly if the script uses a lot of memory. Be careful not to execute scripts with memory leaks.
- The max average using the file manager is 31,180 KB. The uploaded file is 133 MB.

**Network Traffic**

- The max traffic without any connection to the Agent's console is depicted as follows:
  - Max bytes sent per second: 137.

  - Max bytes received per second: 42.
  - Max total bytes transferred per second: 180.
- The max traffic using a remote desktop is depicted as follows:
  - Max bytes sent per second: 469,925.
  - Max bytes received per second: 230,886.
  - Max total bytes transferred per second: 700,811.
- The max traffic using a terminal is depicted as follows:
  - Max bytes sent per second: 16,683.
  - Max bytes received per second: 5,691.
  - Total bytes transferred per second: 22,373.
  - This is a result of using the console command and operations such as ipconfig, ipconfig /all, or netstat. This average may increase significantly if the script sends or receives a lot of data.
- The max traffic using the file manager is depicted as follows:
  - Max bytes sent per second: 533,827.
  - Max bytes received per second: 1,040,282.
  - Total bytes transferred per second: 1,574,109.
  - The uploaded file is 133 MB. These values may change depending on the size of the file to upload/delete and the network bandwidth.

## 10.5 Agent Windows Registry Information

Registry keys created by the Agent's installation depend on the architecture of the Microsoft Windows OS and the Intel® EMA Agent (console and service). These are the registry paths for Intel® EMA Agent by architecture:

- Win64 Service:

  HKEY_LOCAL_MACHINE -> "Software\Intel\EmaAgent"
- Win64 Console:

  HKEY_CURRENT_USER -> "Software\Intel\EmaAgent"

The following registry keys should exist at this reg key root when the Intel® EMA Agent is installed/running:

- **MeshId** - REG_SZ that contains the Endpoint Group ID from the MSH file; if no MSH file is present, then this value will be empty.
- **MeshName** - REG_SZ that contains the Endpoint Group Name from the MSH file; if no MSH file is present, then this value will be empty.
- **NodeId** - REG_SZ that contains the Endpoint ID.

  **NOTE**

  Endpoint ID is tied to the Agent root certificate. Different root certificates are used for service/console.

- **Version** - REG_DWORD that contains the version number of the running EmaAgent.

- **EnhancedLoggingLevel** - REG_DWORD that contains the logging level. By default this is set to 3, which disables enhanced debug logging. To enable enhanced debug logging, edit the registry and set EnhancedLoggingLevel to 4.

# 11.0 Appendix - Performing Intel® EMA Endpoint Operations from a Machine-to-Machine Client Application

The Intel® EMA API supports Machine-to-Machine (M2M) applications performing Intel® EMA in-band and out-of-band endpoint operations directly from the M2M client application. The Intel® EMA API provides a Client Credentials authentication flow to support M2M applications.

First, you will need use the Intel® EMA API to create a Client Credentials account on the Intel® EMA server. This account is used by the M2M client to login to Intel® EMA and request an access token, which allows the client to execute Intel® EMA in-band and out-of-band API calls (referred to as "resources") on the Intel® EMA server. Client Credentials accounts are specific to a particular Tenant. The Client Credentials account can only be created by a Global Administrator user or a Tenant Administrator user of the Tenant in which the Client Credentials account is being created.

**NOTE**

You can create multiple Client Credentials accounts per Tenant.

Once the Client Credentials account is in place, you will need to call the Intel® EMA API from your M2M client application to request an access token. This requires logging in to Intel® EMA using the Client Credentials account. Access tokens are valid for a limited time, and their duration is set as part of the Client Credentials account creation.

Once the M2M client application receives the requested access token, it can make API calls to the Intel® EMA server. For detailed information about the Intel® EMA API, refer Intel® EMA API Guide .

## 11.1 Creating a New Client Credentials Account

To create a new Client Credentials account, login on the Intel® EMA server as a Global Administrator or Tenant Administrator and use the Intel® EMA API for POST api/latest/ClientCredentials, providing the following values:

- **client_secret** - a secret character string of your choice, similar to a password or passphrase. The value must be at least 12 characters, and contain at least one number, both lower and uppercase letters, and at least one special character.
- **maxFailedLogins** - the number of login attempts allowed before the Client Credentials account will be locked. Minimum 5, maximum 15, default 10.
- **tokenLifetimeHours** - the number or hours the token will be valid for. Minimum 1, maximum 24, default 1.

- **tenantID** - the identifier of the tenant for which this Client Credentials account will be created. This is only required for Global Administrators, and can be found by using the api/latest/Tenants API call. For Tenant Administrators, this is not required as its value is automatically the tenantID of the Tenant to which the administrator belongs.
- **scope** - the scope or user role of this client credentials account. This parameter is of type enum, with values "1" or EndpointManager" for the Endpoint Manager role, and "2" or "TenantManager" for the Tenant Manager role. You can enter either the number or the role name. If you enter the role name, note that it is case sensitive and no spaces. If you enter the name incorrectly or enter a number other than 1 or 2 you will get an error message.

## 11.2 API Privileges for Client Credentials Account Scopes

The Client Credentials Tenant Manager has access to APIs that support tenant management. This includes APIs for user management, Endpoint group, Intel AMT Profiles and Intel AMT Setup creation and management.

The Client Credentials Endpoint manager has access to APIs that support performing operations on endpoints. This includes inbound and out of bound operations, endpoint adoption, and unprovisioning.

Consult the swagger documentation to see the full list of supported APIs for each role.

## 11.3 Requesting a Token Using Client Credentials

Once the Client Credentials account is created, use the **POST /api/token** API from your M2M client application to request an access token.

**NOTE**

The **grant_type** must be "client_credentials".

An example of the token API call is shown below:

```
POST /api/token
grant_type=client_credentials
&client_id=xxxxxxxxxx
&client_secret=xxxxxxxxxx
```

Once the M2M client application has executed the token API and received the access token, it can make Intel® EMA API calls for in-band and out-of-band operations directly to the Intel® EMA instance (until the token expires).