



# **Intel® Endpoint Management Assistant (Intel® EMA)**

## **Quick Start Guide**

---

**Intel® EMA Version: 1.6.0**

**Document update date: Tuesday, November 23, 2021**

## Legal Disclaimer

Copyright 2018-2021 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.

---

<b>1 Introduction</b>	<b>1</b>
1.1 High-level architecture diagram	1
<b>2 Supported Operating Systems</b>	<b>2</b>
<b>3 Installation Prerequisites</b>	<b>3</b>
3.1 Computer	3
3.2 Operating System	3
3.3 Database	3
3.4 Web Server	4
3.5 Intel AMT PKI Certificate	5
3.6 Microsoft .NET Framework Versions	5
3.7 Firewall	5
3.8 Network	5
3.9 Network Ports	5
<b>4 Installing or Updating the Intel® EMA Server</b>	<b>7</b>
4.1 Server Host Configuration	7
4.2 Database Settings	7
4.3 Server Host Information	8
4.4 User Authentication	8
4.4.1 Normal Accounts	8
4.4.2 Domain Authentication	9
4.5 Platform Manager Configuration	9
4.6 Global Administrator Account Setup	10
4.7 Summary	10
<b>5 Using the Global Administrator Interface</b>	<b>11</b>
<b>6 Tenant Setup and Endpoint Agent Deployment</b>	<b>12</b>
6.1 Create Your Endpoint Groups	12
6.2 Create Agent Files for Deployment to Managed Endpoints	12
6.3 Create Your Intel® AMT Profiles	13
6.4 Enable Intel® AMT Auto-Setup	14
6.5 Deploying the Agent to Your Endpoints	15
<b>7 Intel® EMA Server Management</b>	<b>16</b>
7.1 Creating New User Groups	16
7.2 Adding, Modifying, and Deleting Users	16
7.3 Assigning Endpoint Groups to User Groups	16
<b>8 Important File and Directory Locations</b>	<b>17</b>

# 1 Introduction

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

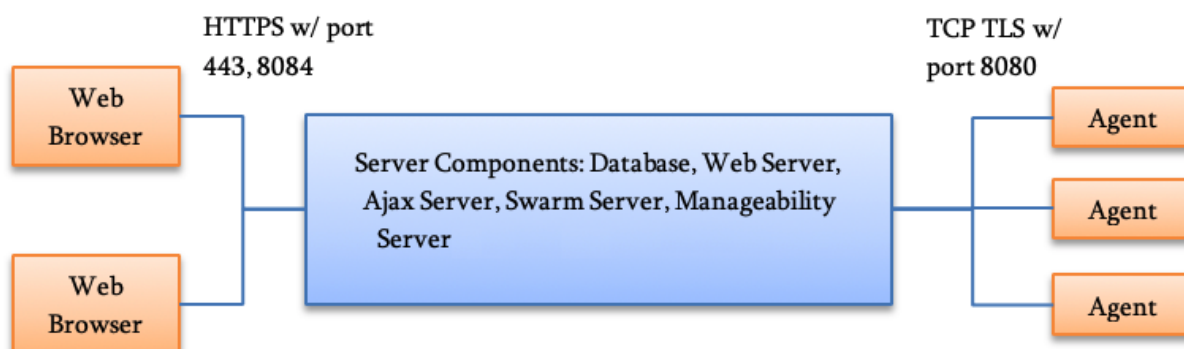
Intel EMA and its management console offer IT a sophisticated and flexible management solution by providing the ability to remotely and securely connect Intel AMT devices over the cloud. Benefits include:

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

This document outlines the necessary steps to install the Intel EMA and helps with some basic configuration to start using the system. This document is intended for use in a tutorial, trial, or proof-of-concept activity, and does not necessarily reflect all the settings and configuration required to implement Intel EMA in a real-world production environment.

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

## 1.1 High-level architecture diagram



## 2 Supported Operating Systems

As a stand-alone application, the Intel® EMA Agent can be installed on the following operating systems:

- Microsoft Windows\* 7 (Intel AMT 11.8 systems only<sup>†</sup>)
- Microsoft Windows 10
- Microsoft Windows 11

Intel EMA Server can be installed on the following operating systems:

- Microsoft Windows Server 2012 R2 (support will end when Intel EMA v1.7.0 is released)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

<sup>†</sup> Windows 7 is supported on Intel AMT 11.8 systems only and will be no longer be supported after Intel AMT 16 is released. Support for Windows 7 and Intel AMT 11.8 will end when Intel EMA v1.7.0 is released.

# 3 Installation Prerequisites

This is a list of the prerequisites needed to set up the Intel® EMA Server.

## 3.1 Computer

A computer or virtual machine with sufficient capability for the expected traffic. Systems not meeting these minimum specifications could experience performance issues.

2 Intel® Xeon® Processors, 16 threads, 24GB RAM, 1TB Mirrored: This configuration should be able to handle over 20k connections.

## 3.2 Operating System

See Supported Operating Systems, section 2.

Currently, Intel EMA does not provide internationalization support. The operating system needs to have English-US Windows display language, English-US system locale, and English-US format (match Windows display language).

## 3.3 Database

Install the Microsoft SQL Server\*. The database may run on a separate server on the network or on the same system as the Intel EMA Server. For demonstration or test purposes, Microsoft SQL Server Express edition can be used if installed with Advanced Features. For production environments, we recommend using Microsoft SQL Server Enterprise. A strong working knowledge of installing, configuring, and using SQL and Active Directory is required (if using 802.1x).



**IMPORTANT:** To achieve security in-depth, we recommend to use Microsoft SQL Server Enterprise and enable Transparent Data Encryption. Additionally Windows authentication mode is recommended as the authentication mode.



### Notes:

- Microsoft SQL Server 2012, 2014, 2016, 2017, and 2019 (English-US version only) are supported. Note that SQL Server 2012 will not be supported once Intel EMA v1.7.0 is released.
- The operating system of the machine on which SQL Server is running must be a supported operating system version and needs to have English-US Windows display language, English-US system locale, and English-US format (match Windows display language). See Supported Operating Systems, section 2.
- The **collation** value in SQL Server must be set to **SQL\_Latin1\_General\_CP1\_CI\_AS**.
- Be sure to allocate enough resources (CPU, memory, SSD, etc.) to SQL Server. If your SQL Server's resources are dynamically allocated, ensure enough guaranteed fixed resources are allocated. If not, you may see error messages like "Unable to get database connection, all connections are busy" in the component server log files in **Program Files (x86)\Intel\Platform Manager\EmaLogs**.
- Intel EMA uses query notification in SQL Server to reduce the number of database reads. That feature requires "Service Broker" to be enabled in SQL server. If Service Broker is disabled, you will see warnings to that effect in the component server log files in **Program Files (x86)\Intel\Platform Manager\EmaLogs**.

- Before installing Intel EMA, ensure that an SQL account exists on the SQL server that can be used by the Intel EMA installer to connect to the SQL server. If you are not the SQL database administrator (SQL DBA), contact the SQL DBA to have this account set up. This account must exist before you install Intel EMA, since you will be asked to specify the SQL connection account during the installation process. This account may be a Windows account under Windows Authentication or an SQL account under SQL Authentication. In addition, the SQL account must have a default database configured. The default database can be any existing database on the SQL server. This default database is required so that the Intel EMA installer can confirm that the specified SQL account/user can contact the SQL server and its databases.
- Before installing Intel EMA, ensure that the SQL account used in the Intel EMA SQL connection string has sysadmin rights (to create new account for IIS default application pool identity) and has at least dbcreator permission, which allows it to create, modify, and delete any database. Also, this account must have the database level roles db\_owner, db\_datawriter, and db\_datareader. The “sysadmin” right is needed in order to create the new user “IIS APPPOOL\DefaultAppPool” for the SQL server (if it does not exist). If it exists already or you do not use that account for the IIS application pool of the Intel EMA website, then the role needed during installation is “dbcreator”, to create the Intel EMA database. Keep in mind that the “sysadmin” or “dbcreator” rights are only needed during Intel EMA installation. Lastly you must grant permission for “SUBSCRIBE QUERY NOTIFICATIONS” to the user of Intel EMA database.



**IMPORTANT:** If you do not grant “sysadmin” rights to the SQL connection account, the installation will still complete successfully, but with errors related to not being able to create the IIS APPPOOL user mentioned above. **If you did not grant “sysadmin” rights to the SQL connection account, you MUST manually create this user on the SQL server after the installation completes in order for Intel EMA to work.**

## 3.4 Web Server

Intel EMA uses Microsoft Internet Information Server (IIS). Use the latest IIS 8, IIS 8.5, or IIS 10 version.

Install IIS URL Rewrite Module for the target IIS. If it is installed, Intel EMA will set up the website setting to remove the IIS server version from the response header, the HSTS header, the cookie Same Site strict, and the auto redirect from HTTP to HTTPS. If it is not installed, these settings will not be applied.



**Note:** If IIS is already installed, ensure that all authentication methods are disabled except for “Anonymous” and “Windows” (only those two should be enabled). This only applies to Windows Authentication mode.

Authentication		
Group by: No Grouping		
Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

## 3.5 Intel AMT PKI Certificate

Intel AMT Admin Control Mode (ACM) provisioning requires a certificate issued by a trusted authority that matches the domain name of the target Intel AMT endpoints. 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).

## 3.6 Microsoft .NET Framework Versions

Intel EMA Server software is built with Microsoft .NET Framework 4.8. The operating system must have Microsoft .NET Framework 4.8 or later. If .NET Framework 4.8 or later is not installed, the Intel EMA installer will display a dialog prompting you to download and install .NET Framework 4.8 runtime.

## 3.7 Firewall

We recommended using a firewall software to ensure that only authorized ports are available for connection. The firewall software built into Windows can perform this task.

## 3.8 Network

During the installation, you must specify the value (either hostname or IP address) to use for communication among various components. If you choose hostname or FQDN, you need to make sure the value is resolvable by a DNS server in the network. If you do not have the DNS server, a fixed IP address should be used during installation. Incorrect hostname/IP address will cause Intel EMA features to not function properly. In a distributed server architecture implementation, if using Active Directory, ensure all computers (including the computer hosting the load balancer) are listed in Active Directory.

## 3.9 Network Ports

Table 1 lists the server network ports used for various communications among server components.

- For certain features/usages, the AJAX server and Manageability server will establish a TCP connection (locally or remotely) with the Swarm server.
- The endpoint and the Swarm server communicate via a secure TCP connection. Intel AMT (CIRA) and the Swarm server communicate via a secure TCP connection.
- The Platform Manager service uses a named pipe to talk to other Intel EMA component servers on the same machine. The Platform Manager client application talks to the Platform Manager service via a secure TCP connection.

**Table 1: Server network ports**

Protocol	Port	Usage
TCP	443	HTTPS Web server port. This is used between the web browser and the web server.
TCP	1433	SQL server remote access. This is used between the internal Intel EMA server and the internal SQL server; only needed if Intel EMA server and the SQL server are not on the same machine. This is the default port that SQL server uses.
TCP	8000	The default TCP port for communication between Platform Manager

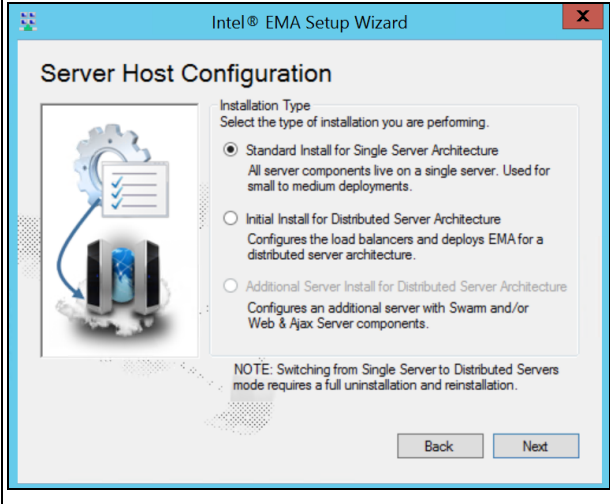


		service and Platform Manager client. You can change this port during installation.
TCP	8080	Agent, console, and Intel AMT CIRA port. This is between client endpoints and the Intel EMA Swarm server. See note below.
TCP	8084	Web redirection port. This is used between the web browser and the web server.
TCP	8089	Communication between the various Intel EMA component servers and Intel EMA Swarm server. This port number is the default, and can be changed in the Server Settings page.
TCP	8092	Port on which Ajax component server listens for internal component-to-component communication. This port number is the default, and can be changed in the Server Settings page.
TCP	8093	Port on which Swarmcomponent server listens for internal component-to-component communication. This port number is the default, and can be changed in the Server Settingspage.
TCP	8094	Port on which Manageability component server listens for internal component-to-component communication. This port number is the default, and can be changed in the Server Settings page.
LDAPS/LDAP	636/389	The LDAPS secure port is 636. The standard non-secure LDAP port is 389. These ports are for use with Active Directory and/or 802.1x configuration.
Global Catalog (secure/non-secure)	3269/3268	The secure (3269) and non-secure (3268) Global Catalog ports. These ports are for use with Active Directory and/or 802.1x configuration.

# 4 Installing or Updating the Intel® EMA Server

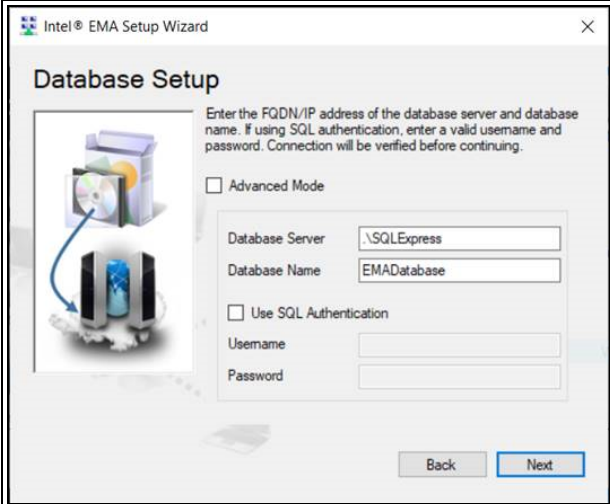
Follow the steps below to install the Intel® EMA server.

## 4.1 Server Host Configuration




Choose **Standard Install for Single Server Architecture**.

## 4.2 Database Settings



Specify the server where the database is hosted. The actual value depends on the database server you installed. Refer to your SQL installation for details.

 **Notes:**

- If you are using a SQL server installed on the same machine as Intel® EMA then you can use localhost.
- If you are using a remote SQL server, ensure the SQL server's account is set up for your IIS Default Application Pool to connect.
- For security purposes, we recommend that Windows authentication mode is used for SQL Authentication. If using SQL Authentication, you must ensure the target credential is set up in the SQL server first.

## 4.3 Server Host Information

The screenshot shows the 'Server Host Information' window of the Intel® EMA Setup Wizard. It includes a sidebar with a server icon and a main area with instructions: 'Use this screen to enter the information about the machine on which you are installing Intel® EMA. The FQDN or IP address you enter here will be the URL by which the Intel® EMA website will be accessed.' The form fields are: 'FQDN/Hostname' (with a masked value), 'IP Address' (with a masked value), 'Identity mode' (set to 'Use FQDN/hostname only'), and 'Additional Names' (containing 'localhost' and a masked value). 'Back' and 'Next' buttons are at the bottom.

If you have a Website TLS certificate for the server, enter a matching hostname for the server here.

This is the main Intel® EMA website HTTPS URL, and this is the FQDN/hostname that will be provided in the agent configuration file for endpoints to connect to, so make sure that it resolves correctly in DNS.

### For Identity mode:

- **Use FQDN/hostname only:** processes the request with the FQDN/hostname only. We suggest entering the addressable, full FQDN.
- **Use FQDN/hostname first:** processes the request using the FQDN/hostname, but can also find the website via the IP Address.
- **Use IP address:** processes requests with the IP address only



**Note:** If Intel EMA will be installed under domain/Windows authentication mode (Kerberos) in the next step, we recommend using the FQDN of your machine at Hostname field. You still need to ensure that other endpoints or other client web browsers can connect to the value you entered here. If you decide to use another value, follow IT best practices to set up the Service Principle Name (SPN) after Intel EMA is installed. Choosing Use IP address does not work for Kerberos.

## 4.4 User Authentication

Choose either **Use normal accounts** or **Use domain authentication**.

### 4.4.1 Normal Accounts

The screenshot shows the 'User Authentication Type' window of the Intel® EMA Setup Wizard. It includes a sidebar with a server icon and a main area with instructions: 'This server has been detected to be part of a domain. Select what type of user authentication will be used on this server. If domain authentication is used, the currently logged in user will be the first global administrator.' The form has a 'User Authentication' section with a 'User Identity' dropdown menu set to 'Use normal accounts'. 'Back' and 'Next' buttons are at the bottom.

If you select Use normal accounts then Intel® EMA will keep an internal user database.

This is the default setting of the installation process. This puts the installed instance in username/password mode.

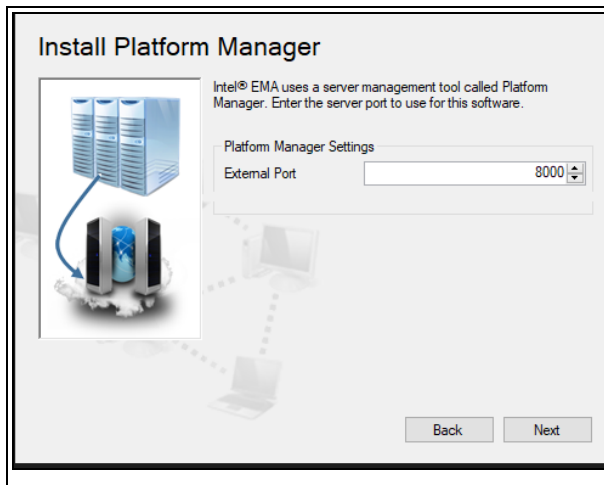
## 4.4.2 Domain Authentication



If your server is joined to an Active Directory domain, you have the option to Use domain authentication.

The currently logged-in user is automatically added to Intel EMA with the Global Administrator role (shown as Site Administrator in the screen at left).

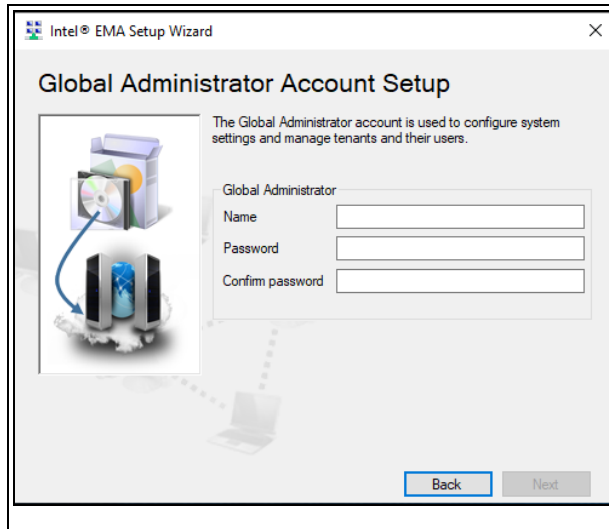
## 4.5 Platform Manager Configuration



**External Port** is used by the Intel® EMA Platform Manager service running on this Intel EMA server to accept connection from the Intel EMA Platform Manager client application. Make sure that the port you specify is open in the underlying network.

This screen cannot be edited in update mode.

## 4.6 Global Administrator Account Setup



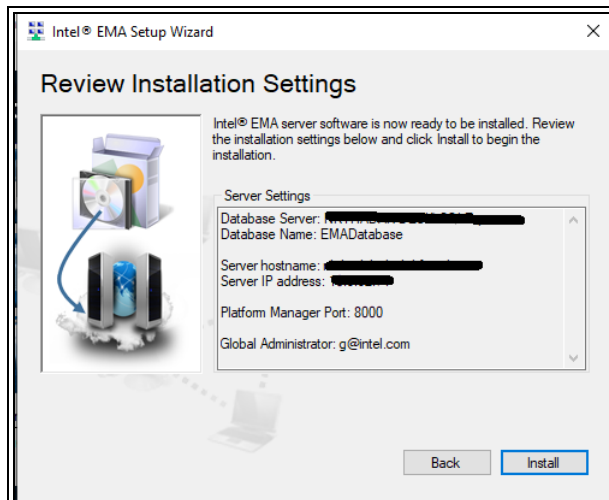
This screen only appears during setup if you have chosen “Normal accounts” for user authentication. If using domain accounts, the user running the installer will be made a Global Administrator.



**Note:** The **Name** field must be entered in the form of an email address (i.e., name@domain).

**Global Administrator:** This role is able to perform user management, tenant creation, and server management. This role does not perform device management.

## 4.7 Summary



Review your installation settings and then click **Install**.

All required Windows components will be installed, followed by the Intel® EMA software itself.



**IMPORTANT:** Do not abort or exit the installer until installation is complete. Installation rollback is not supported.

Installation status is shown at the bottom of the Installer main menu. Installation options are unavailable during installation.

To check the log file during installation, click **File > Advanced Mode**. To exit Advanced Mode, click **File > Advanced Mode** again.

After installation, you can check the logfile **EMALog-Intel®EMAInstaller.txt** in the same folder as the Intel EMA installer.

At this point, you are ready to log in as the Global Administrator and click **View Getting Started tips** under **Getting Started** on the overview page. See section 5.

# 5 Using the Global Administrator Interface

Intel® EMA's Global Administrator pages are used to manage tenants, users, and user groups.

To login to Intel EMA, do the following:

1. Open a browser and navigate to the FQDN/Hostname you specified during installation.
2. At the login page, enter the user name (i.e., email address) and password for the Global Administrator.



**Note:** If you specified domain authentication, the Global Administrator Overview page is automatically displayed.

1. At the bottom of the **Overview** page, under **Getting Started**, click **View Getting Started tips**.
2. On the **Getting started** page, follow the steps (in order) to **Create a Tenant**, **Add a Tenant Administrator**, and then **Add Additional Users** (if desired). Note that you **MUST** create at least one Tenant Administrator for each Tenant you create. The Global Administrator cannot perform many of the tasks in Tenants.

## Logging out

To log out, click the user name in the top bar of the **Overview** page and select **Log out**.

# 6 Tenant Setup and Endpoint Agent Deployment

This section describes how to set up your Tenant work space on the Intel® EMA server and deploy the Intel EMA agent to your managed endpoint systems.



**Note:** You must be logged in to the Intel EMA server as a user with Tenant Administrator privileges to perform the steps in this section.

To login to Intel EMA, do the following:

1. Open a browser and navigate to the FQDN/Hostname specified during server installation.
2. At the login page, enter the user name (i.e., email address) and password for the Tenant Administrator user.

## 6.1 Create Your Endpoint Groups

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. Click **Generate agent installation files**.

### Endpoint Group Setup

Define the policy and enable Intel® AMT auto-setup (optional) -- for a group of endpoints.

1 Define the group

2 Generate agent installation files

1 Create a new group

Group Name  
new group

Group Description  
description here

Password (required to change the policy later)  
.....

.....

[Save & Intel® AMT autosetup](#)

2 Group Policy

Enable Intel® EMA users with execute rights to use these capabilities on the group:

**Power operations**

☐ Wakeup

☐ Sleep

☐ Turn off or restart

**Messaging and alerts**

☒ TCP traffic relay

☐ Alert messages

☐ Console prompts

☐ Location information

☒ Peer-to-peer communication

**Remote control**

☐ Remote KVM

☐ Remote file access

☐ Remote management (WMI)

☐ User Consent for In-Band KVM

[Select all](#)

[Generate agent installation files](#)

## 6.2 Create Agent Files for Deployment to Managed Endpoints

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. Select the platform that you want to use (32-bit or 64-bit).
3. Click **Download** for the Agent policy file, then click **Done**.

### Generate Agent Installation Files

After the files are installed on endpoints, the endpoints will join this group:

Choose your endpoint platforms and download the agents for them

- ☐ Windows (32-bit) Service
- ☐ Windows (64-bit) Service

Also download the agent policy file

Agent policy file [Download](#)

Now, go copy the agent policy file and the appropriate agent file to each endpoint (manually or using a distribution tool).

Install the agent by running the agent as administrator for that endpoint

Tip: keep the agent and agent policy files together. The file names (other than the extensions) must be the same

[Done](#)

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.

## 6.3 Create Your Intel® AMT Profiles

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**.

If you specify CIRA, take note of the following:

- 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.

- 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.



Figure 1: Create a profile – General settings

The screenshot shows the 'New Intel® AMT profile' dialog box with the 'General' tab selected. On the left is a sidebar menu with options: General, Power States, Management Interfaces, FQDN Source, IP Address, WiFi, and Wired 802.1X. The main area contains fields for 'Profile Name' and 'Profile Description' (with a help icon). Below these is a section for 'Use Client Initiated Remote Access (CIRA)' which is selected. A tip states: 'Tip: If the computer is behind an HTTP proxy, use TLS security instead.' There is a field for 'CIRA intranet suffix:' with a placeholder 'Suffix from your intranet (example: mydomain1.com)'. Below that is a 'CIRA Proxy Settings' table with columns 'Proxy DNS Suffix', 'Access Info', and 'Port'. The table is currently empty, showing 'No settings added'. An 'Add' button is to the right of the table. At the bottom, there is an option 'Use TLS security' which is not selected. 'Save' and 'Cancel' buttons are at the bottom right.

Proxy DNS Suffix	Access Info	Port
No settings added		

## 6.4 Enable Intel® AMT Auto-Setup

1. Select the **Enabled** checkbox and choose the **Intel® AMT profile** you created previously.
2. Select the **Activation Method** to be used. For quick start, use **Host Based Provisioning**.
3. 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.
4. Click **Save**.
5. If you are performing an initial Tenant setup, proceed to section 6.5 to deploy the agent files to your endpoints.

**Intel® AMT autosetup** (EpG01)

After setting up, any endpoint joining this group and supporting Intel® AMT will automatically be activated. Need to have at least 1 Intel® AMT profile.

☒ Enabled

Intel® AMT profile: Prof01

Activation Method: Certificate Provisioning (TLS-PKI) ?

Administrator Password:  ☐ display ?

Intel® MEBX Password Configuration ?

☒ Set a random password per endpoint (recommended)  
☐ Do not set the password (not recommended)

Certificates Details:
 

Available Certificates:  
 Cert01  
 Domain:  
 unite4.vprodemo.com

Save Cancel

## 6.5 Deploying the Agent to Your Endpoints

### 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

### 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.

# 7 Intel® EMA Server Management



**Note:** To perform the steps in this section, log on to the Intel® EMA server as the Tenant Administrator user. For information about user roles and the difference between Global Administrator and Tenant Administrator users, see User Roles in the *Intel® EMA Administration and Usage Guide*.

## 7.1 Creating New User Groups

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 which level of permission to grant to the users in this User Group.



### Notes:

- The **New Group** button 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. Click **Endpoint Groups** and select the Endpoint Groups to which this User Group will have access.

## 7.2 Adding, Modifying, and Deleting Users

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.

## 7.3 Assigning Endpoint Groups to User Groups

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

## 8 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 <ul style="list-style-type: none"><li>• EMALog-XXX.txt</li><li>• TraceLog-XXX.txt</li></ul>	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. For 32 bit agent, see Program Files (x86).
C:\inetpub\wwwroot	IIS web site locations.