



Intel® Endpoint Management Assistant (Intel® EMA)

Quick Start Guide

Rev. 1.14.0

August 2024

Legal Disclaimer

Copyright 2018-2024 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 | 6 |
| 1.0 Introduction | 7 |
| 2.0 Supported Operating Systems | 9 |
| 3.0 Installation Prerequisites | 10 |
| 3.1 Computer..... | 10 |
| 3.2 Operating System..... | 10 |
| 3.3 Database..... | 10 |
| 3.4 Pre-installation Instructions for Microsoft Azure AD Environments..... | 12 |
| 3.5 Web Server..... | 13 |
| 3.6 Intel® AMT PKI Certificate..... | 14 |
| 3.7 Microsoft .NET Framework Versions..... | 14 |
| 3.8 Firewall..... | 14 |
| 3.9 Network..... | 14 |
| 3.10 Network Ports..... | 15 |
| 4.0 Installing Using the Setup Wizard | 17 |
| 4.1 Initial Server Installation..... | 17 |
| 4.1.1 Server Host Configuration..... | 18 |
| 4.1.2 Database Settings..... | 19 |
| 4.1.3 Load Balancer Information..... | 21 |
| 4.1.4 Server Components to Deploy..... | 23 |
| 4.1.5 Platform Manager Configuration..... | 23 |
| 4.1.6 User Authentication..... | 23 |
| 4.1.7 Global Administrator Account Setup..... | 25 |
| 4.1.8 Finishing Up..... | 26 |
| 4.1.9 Summary..... | 27 |
| 4.1.10 Modify Server Settings for Azure AD..... | 27 |
| 5.0 Using the Global Administrator Interface | 29 |
| 6.0 Tenant Setup and Endpoint Agent Deployment | 30 |
| 6.1 Create Your Endpoint Groups..... | 30 |
| 6.2 Create Agent Files for Deployment to Managed Endpoints..... | 31 |
| 6.3 Create Your Intel AMT Profiles..... | 32 |
| 6.4 Enable Intel AMT Auto-Setup..... | 33 |
| 6.5 Deploying the Agent to Your Endpoints..... | 34 |
| 7.0 Intel® EMA Server Management | 35 |
| 7.1 Creating New User Groups..... | 35 |
| 7.2 Adding, Modifying, and Deleting Users..... | 35 |
| 7.3 Assigning Endpoint Groups to User Groups..... | 35 |
| 8.0 Important File and Directory Locations | 37 |



Figures

- 1 Endpoint Group Setup Page..... 31
- 2 Generate Agent Installation Files 32



Tables

| | | |
|---|---------------------------|----|
| 1 | Server Network Ports..... | 15 |
|---|---------------------------|----|

Revision History

| Revision Number | Description | Release Date |
|-----------------|----------------------|--------------|
| 1.14.0 | Revision update only | August 2024 |

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 the procedure to install and configure the Intel® EMA server in a full production environment, as well as how to maintain and manage the Intel® EMA server after installation. It is intended for technically competent system administrator users working with Intel® EMA in the Global Administrator role.

NOTE

A simplified tutorial installation procedure for learning purposes is available in the Intel® EMA Quick Start Guide.

The Global Administrator is responsible for installation, configuration, and management of the Intel® EMA server as a whole, as well as creating Tenant usage spaces within the Intel® EMA server. Other Intel® EMA users, such as Tenant Administrators and Account Managers are responsible for setting up and maintaining the users, user groups, endpoint groups, and managed endpoint client systems for each Tenant hosted on the Intel® EMA server.

NOTE

Key concepts such as user roles, tenants, and endpoint groups are described in detail in the Intel® EMA Administration and Usage Guide, which also provides detailed information about the setup and maintenance of Intel® EMA Tenants and their managed endpoint systems.

We recommend that you read this guide carefully before performing the installation. This document provides the installation requirements, explains the configuration parameters, and provides detailed installation steps for the Intel® EMA server and its components.

2.0 Supported Operating Systems

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

- Microsoft Windows 10
- Microsoft Windows 11

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

- Microsoft Windows Server 2019

NOTE

The getPFX API requires the Intel® EMA server to be installed on Windows Server 2019 or later

- Microsoft Windows Server 2022

NOTE

Crypto for Intel ME 11 systems is disabled by default on Windows Server 2022

3.0 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

Refer Supported Operating Systems

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 2017, 2019, and 2022 (English-US version only) are supported.
- 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). Refer Supported Operating Systems.
- 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**.
- If you choose SQL authentication during installation you will be required to supply two database connection strings. One string is for a more permissive account used to install the database, and the other is for less permissive account used by Intel® EMA services to access the database after installation.
- Before installing Intel® EMA, ensure that an account exists on the SQL server that can be used by the Intel® EMA installer to connect to the SQL server and create the Intel® EMA database. 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 to create the database 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.**

Refer Security Recommendations for information about changing these permissions and roles

3.4 Pre-installation Instructions for Microsoft Azure AD Environments

If you plan to install Intel® EMA in an existing Microsoft Azure AD environment, follow the steps below in order to enable Intel® EMA to successfully connect to the Azure AD environment. We recommend that you perform these steps before installing Intel® EMA, however they can be performed after installation, though you will not be able to add users and perform other Intel® EMA actions until you perform these steps in Azure AD.

NOTE

Intel® EMA instances configured to use Azure AD authentication do not support individual user authentication via the REST API from scripts or outside applications. Use of Client Credential authentication is a supported alternative on these instances. If you require the use of integrating applications or administrative scripts that call Intel® EMA's APIs, verify that they will work with Azure AD authentication before proceeding with a production deployment.

1. In your Azure AD tenant (note that this is NOT the same as an Intel® EMA tenant), create a new app registration. This app will be associated with Intel® EMA once Intel® EMA is installed, and Intel® EMA will use this app to interact with Azure AD to exchange information.
 - a. Go to **Azure Active Directory > App Registration** and create a new app registration.
 - b. **Supported account types** for the new app must be **Accounts in this organizational directory only**.
 - c. Configure the Redirect URI, choosing Web as the Platform.
 - d. Enter `https://<EMA FQDN or IP>/api/latest/azureLogin` as the **Redirect URL** value.
-

NOTE

This URL is case sensitive

2. In the **Certificates & Secrets** section for the newly registered app, add a new client secret:

- a. At the time of client secret creation, record the client secret's value, as it is only displayed once. You will need this value later when you configure Intel® EMA's Web Server settings after installation. Be sure to secure this sensitive information.
 - b. Consider the expiration date for the client secret. Note that before it expires, you will need to create a new client secret and update the Web Server settings in Intel® EMA.
3. In the API permissions section for the newly registered app, add the required permissions:
 - a. Ensure that a "Delegated" permission type for **Microsoft Graph** with "User.Read" permission exists.
 - b. Add a permission for **Microsoft Graph** with "Application" Type and with "User.Read.All" permission.
 - c. Click to **Grant admin consent** for these API permissions.
 4. Go to **Overview** section of the newly registered app and copy/record the Azure AD Directory (tenant) ID, the Azure AD Application (client) ID, to go with the Azure AD Client Secret Value you created above. Use these values to configure the Intel® EMA Web Server after initial server installation, as described in [#unique_10](#)

3.5 Web Server

Intel® EMA uses Microsoft Internet Information Server (IIS). Use the latest 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. Further, the rewrite module will add 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.

| 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 |

3.6 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).

NOTE

Starting with Intel ME 15 systems support for SHA1 root certificates or RSA key sizes smaller than 2048 in Intel AMT PKI Certificate chain was removed.

3.7 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.

3.8 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.

3.9 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.

FQDN and/or IP addresses selected are used for various purposes:

- Swarm Server Load Balancer FQDN/IP address is the location that will be provided in the agent configuration file for endpoint agents, Intel AMT, or Intel® Standard Manageability to connect to.
- Ajax & Web Server Load Balancer FQDN/IP address is used for the main Intel® EMA website HTTPS URL.
- Recovery Server Load Balancer FQDN/IP address is used to support One Click Recovery.

These settings CANNOT be changed after installation. Make sure each resolves correctly in DNS, and consider choosing a FQDN that can be flexibly reconfigured to a different server when needed – for example, a dynamic DNS entry.

3.10 Network Ports

Table below 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 | 8083 | Web redirection port. This is used between the web browser and the web server. |
| TCP | 8085 | Recovery port. This is used by the Recovery component server. If you change this port on the Recovery Server tab of the Server Settings page, you will be prompted to update port bindings. Refer #unique_17 |
| 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. Refer #unique_17 |
| 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. Refer #unique_17 |
| TCP | 8093 | Port on which Swarm component server listens for internal component-to-component communication. This port number is the default, and can be changed in the Server Settings page. Refer #unique_17 |
| 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. Refer #unique_17 |
| TCP | 8095 | Port on which Recovery component server listens for internal component-to-component communication. This port number is the default, and can be changed in the Server Settings page. |

continued...

| Protocol | Port | Usage |
|------------------------------------|-----------|--|
| | | Refer #unique_17 |
| 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. |

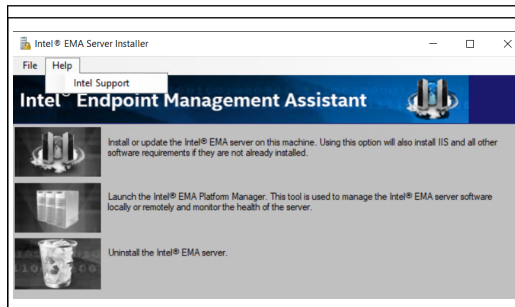
† You can change the port that the agent and Intel® AMT CIRA use to connect to the Intel® EMA server.

- On the load balancer, create a forwarding rule to route the desired port (for example, 8081) to the backend Swarm server port 8080. **Note** the Swarm server is still listening on port 8080, but this allows you to set a different port for your external facing network.
- On the Manageability server, change server settings **ciraserver_port** from 8080 to the desired port (i.e., 8081 in this example). Halt and restart the Manageability server. Refer [#unique_17](#) for information about changing settings for Intel® EMA component servers.
- For web server settings, change server settings SwarmServerPort from 8080 to desired port. Sync the IIS app setting with this change. Refer [#unique_17](#) for information about changing settings for Intel® EMA component servers.
- Create a new endpoint group (note that the existing endpoint group will not have the new SwarmServerPort information) and register an endpoint to this new endpoint group. Then provision Intel AMT on the endpoint. Refer Intel® EMA Administration and Usage Guide for information about endpoint groups and provisioning Intel® AMT on endpoints.

4.0 Installing Using the Setup Wizard

Follow the steps below to install the Intel® EMA server in a distributed architecture installation.

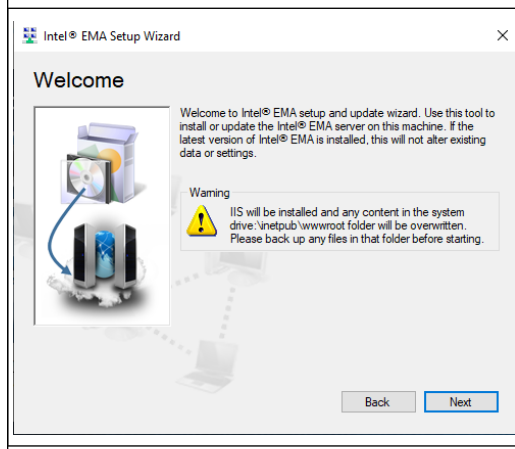
4.1 Initial Server Installation



Extract the installation ZIP file, open the folder, and right-click on EMAServerInstaller.exe and select **Run as administrator**. The installer opens and the status bar at the bottom shows Ready if the initial checks have passed.

Click the top-left icon to begin the installation process.

Note: For assistance, click **Help > Intel Support**



Warning: For first-time installations, if you continue with the installation process, the Intel® EMA Setup Wizard will delete everything in the c:\inetpub\wwwroot folder. Be sure to backup any needed files before continuing with the installation process.

This does NOT apply when updating from a previous Intel® EMA version, although IIS bindings will be set to default values.

Click **Next** on the Welcome screen to continue the setup process. When the License Agreement is displayed, accept the license to continue.

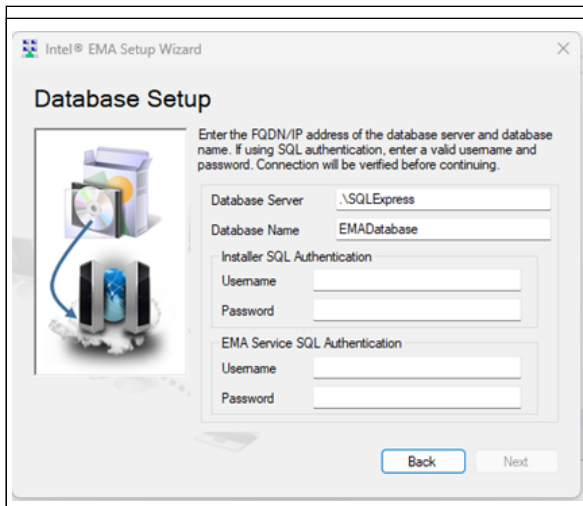
Click **Next** on the Welcome screen to continue the setup process.

4.1.1 Server Host Configuration

| | |
|--|---|
| | <p>Initial Install for Distributed Server Architecture</p> <p>One or more of the server components are installed on this server machine, and additional instances of components can be installed on different server machines using the Additional Server Install option below.</p> <p><i>Note:</i> If you are installing all components on one machine, you do not need to perform the steps in the Additional Server Install section.</p> |
|--|---|

4.1.2 Database Settings

| | |
|--|--|
| | <p>Select the desired authentication type: Windows Authentication, SQL Authentication, or Advanced Mode.</p> <p><i>Note:</i> 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.</p> |
| | <p>If you chose Windows Authentication the account you are using for installation will be used to authenticate against the SQL server and create the database.</p> <p>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.</p> <p>When the installation of Intel® EMA is complete you can change the account used to access the database by modifying the service settings for the Intel Platform Manager service in the Windows Services settings.</p> |



If you chose SQL Authentication or Advanced Mode you will need to enter two sets of credentials.

- Note:**
- These two accounts must be created ahead of time by a system administrator
 - One used by the installer which requires either db_owner, sysadmin, or db_creator permissions.
 - One for the Intel® EMA services to use after installation, which allows the database service to be run with lesser privileges.
 - This account must be granted rights to connect to the Intel® EMA database and granted execute permissions for the dbo, manageability, and security schemas.
 - If the account used by the Intel® EMA services is granted the sysadmin role, and that is later removed, access to the database will no longer work.
 - 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.

SQL Authentication:

- 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.
- Specify the SQL Server accounts that will be used to create the database and the account that will be used by the Intel® EMA services to access the database after installation is complete.

Advanced Mode:

- Specify two customized database connection strings. One for installation of the database, and one for the Intel® EMA services to use after the Intel® EMA installation is complete.

For more information about connection strings, refer <https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax>. Note that some examples on this page may not be supported by Intel® EMA.

| | |
|--|--|
| | <p><i>Note:</i> The parameter "MultipleActiveResultSets=True" is required. For more information, refer https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/sql/enabling-multiple-active-result-sets.</p> <p>The connection string is encrypted and stored in c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config.</p> <p><i>Important:</i> If installing a distributed server architecture, copy the customized connection strings to a text file to save it for use when installing additional servers.</p> <p><i>Note:</i> During an upgrade, the connection information is displayed but cannot be edited as part of the installation flow.</p> |
|--|--|

4.1.3 Load Balancer Information

| | |
|--|--|
| | <p>For Identity mode:</p> <ul style="list-style-type: none"> • Use FQDN only: processes the request with the FQDN only. We suggest entering the addressable, full FQDN. • Use FQDN first: processes the request using the FQDN, but can also find the website via the IP Address. • Use IP address: processes requests with the IP address only <p><i>Note:</i> A full FQDN is required to use the One Click Recovery capability of Intel AMT. If you plan to use the One Click Recovery feature, you must enter a complete FQDN (server_name.domain), not just a host name. Also, do not select Use IP Address if you plan to use One Click Recovery.</p> <p>Intel AMT relies on DNS lookups to resolve remote hosts. If you choose to use a short name/host name for your server instead of a DNS resolvable FQDN, Intel AMT remote management functionality may not work correctly.</p> <p>Enter the FQDN and/or IP Address (or both, depending on Identity mode) of the load balancer for the Swarm Server.</p> <p style="text-align: right;">continued...</p> |
|--|--|

| | |
|--|---|
| | <p>Note: If you are installing all Intel® EMA server components on the same machine (or VM), enter the FQDN and/or IP Address of the machine or VM on which you are installing Intel® EMA.</p> |
| | <p>Enter the FQDN and/or IP Address (or both, depending on Identity mode) of the load balancer for the Ajax Server and Web Server components (or select Same as Swarm Server).</p> |
| | <p>Enter the FQDN and/or IP Address (or both, depending on Identity mode) of the load balancer for the Recovery Server component (or select Same as Swarm Server).</p> |

NOTE

If you plan to use domain/Windows authentication mode (Kerberos), you will need to set up a Service Principle Name (SPN) for the load balancer that supports the Ajax and Web server(s).

4.1.4 Server Components to Deploy

| | |
|--|--|
| | <p>Specify which server components to deploy on this server machine, then verify the IP Address of this server machine (field filled in by default).</p> <p><i>Note:</i> Only one machine can run the Manageability Server component.</p> |
|--|--|

4.1.5 Platform Manager Configuration

| | |
|--|---|
| | <p>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.</p> <p>This screen cannot be edited in update mode.</p> |
|--|---|

4.1.6 User Authentication

Choose which form of authentication you wish to use.

4.1.6.1 Local Accounts



If you select **Use local 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.

4.1.6.2 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).

4.1.6.3 Azure Active Directory Authentication



If your IT environment includes Azure Active Directory, you have the option to choose **Use Azure AD Authentication**. This option allows you to enter a username and password for the first account with Global Administrator role. This account does not need to be in Azure Active Directory. After installation, you can use this account to log in and create the subsequent users, which must be in Azure Active Directory.

4.1.7 Global Administrator Account Setup

Intel® EMA Setup Wizard

Global Administrator Account Setup

The Global Administrator account is used to configure system settings and manage tenants and their users.

Global Administrator

Name

Password

Confirm password

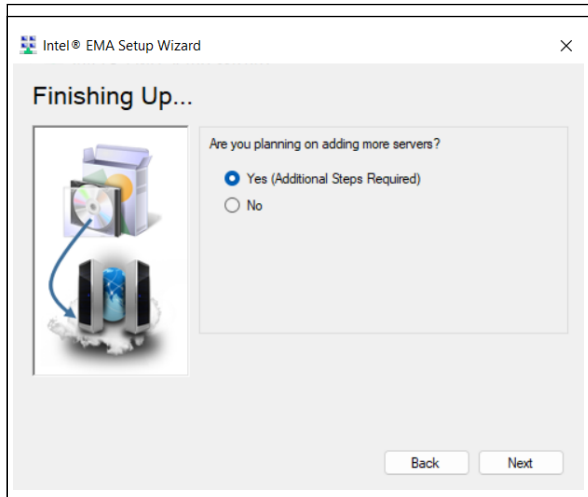
Back Next

This screen only appears during setup if you have chosen "Normal accounts" or "Azure AD Authentication" 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. In Azure AD environments, this user account is needed for configuring Intel® EMA as described in [Modify Server Settings for Azure AD](#) on page 27

4.1.8 Finishing Up



Intel® EMA Setup Wizard

Finishing Up...

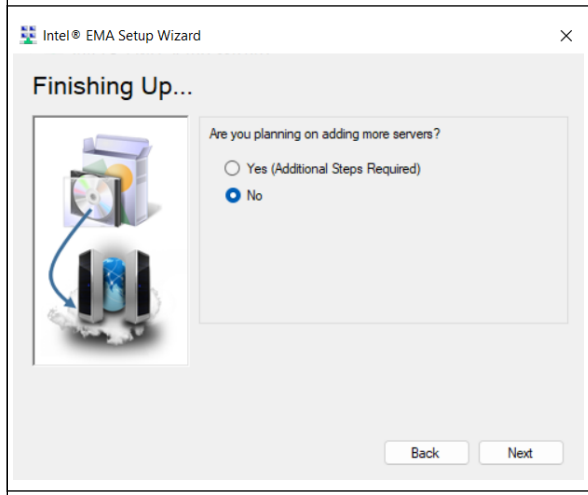
Are you planning on adding more servers?

Yes (Additional Steps Required)

No

Back Next

Select No at this screen.



Intel® EMA Setup Wizard

Finishing Up...

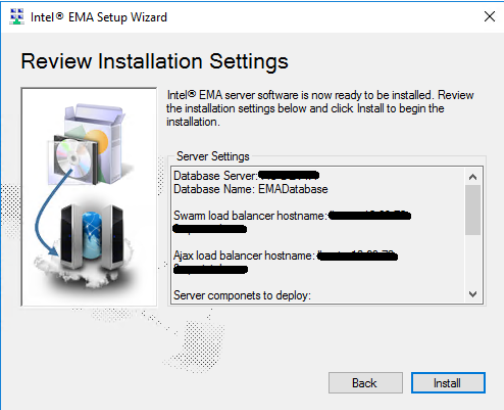
Are you planning on adding more servers?

Yes (Additional Steps Required)

No

Back Next

4.1.9 Summary

| | |
|---|---|
|  | <p>Review your installation settings and then click Install.</p> <p>All required Windows components will be installed, followed by the Intel® EMA software itself.</p> <p><i>Important:</i> Do not abort or exit the installer until installation is complete. Installation rollback is not supported.</p> <p>Installation status is shown at the bottom of the Installer main menu. Installation options are unavailable during installation.</p> <p>To check the log file during installation, click File > Advanced Mode. To exit Advanced Mode, click File > Advanced Mode again.</p> <p>After installation, you can check the logfile EMALog-Intel®EMAInstaller.txt in the same folder as the Intel® EMA installer.</p> |
|---|---|

NOTE

The following warning appears in the installation log file regardless of whether you are installing with a local SQL Server or a remote SQL Server. For installations with a remote SQL Server, this message can be ignored. For local SQL server installations, ensure the the account is set up to allow your IIS Default Application Pool to connect.

```
EVENT: DbWarning, ExecuteNonQuerySafe warning: CREATE LOGIN [IIS
APPPool\DefaultAppPool] FROM WINDOWS () -
System.Data.SqlClient.SqlException (0x80131904): User does not
have permission to perform this action.
```

4.1.10 Modify Server Settings for Azure AD

NOTE

These steps are only needed if you installed Intel® EMA using Azure AD authentication mode.

The following steps are performed on the Server Settings tab of the Intel® EMA user interface. These steps must be performed before you can add additional users in Azure AD authentication mode.

1. Login to Intel® EMA using the initial Global Administrator (root GA) account with its username and password.
2. Navigate to the Server Settings page, then the Web Server settings.
3. Using the values that you copied and saved in [Pre-installation Instructions for Microsoft Azure AD Environments](#) on page 12, enter the **Azure AD Directory (tenant) ID**, the **Azure AD Application (client) ID**, and the **Azure AD Client Secret Value**.

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.

When these settings are updated the Intel® EMA Server will do a test to verify a connection to the Azure AD environment is successful.

5.0 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.

3. At the bottom of the **Overview** page, under **Getting Started**, click **View Getting Started tips**.
4. 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**.

6.0 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**.

Figure 1. Endpoint Group Setup Page

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 [Save & Intel® AMT autosetup](#)

Group Name ?

Group Description ?

2 Group Policy

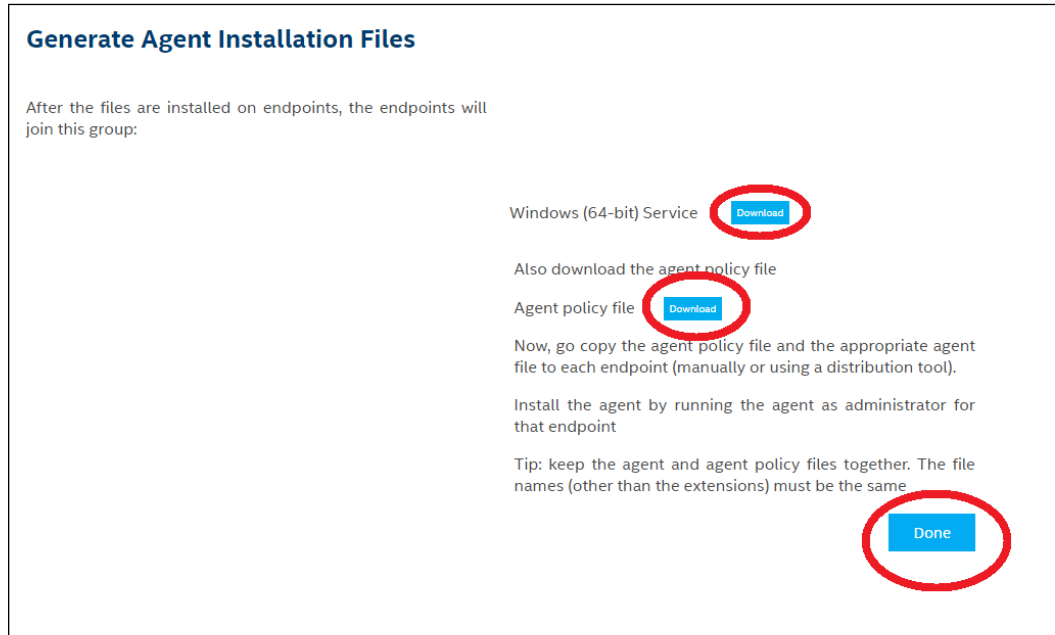
Enable Intel® EMA users with execute rights to use these capabilities on the group:

| | | |
|---|---|---|
| <p>Power operations</p> <p><input type="checkbox"/> Wakeup</p> <p><input type="checkbox"/> Sleep</p> <p><input type="checkbox"/> Turn off or restart</p> | <p>Messaging and alerts</p> <p><input checked="" type="checkbox"/> TCP traffic relay</p> <p><input type="checkbox"/> Alert messages</p> <p><input type="checkbox"/> Console prompts</p> <p><input type="checkbox"/> Location information</p> <p><input checked="" type="checkbox"/> Peer-to-peer communication</p> | <p>Remote control</p> <p><input type="checkbox"/> Remote KVM</p> <p><input type="checkbox"/> Remote file access</p> <p><input type="checkbox"/> Remote management (WMI)</p> <p><input type="checkbox"/> User Consent for In-Band KVM</p> |
|---|---|---|

[Select all](#)

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. Click **Download** for the Windows 64-bit Service agent file.
3. Click **Download** for the Agent policy file, then click **Done**.

Figure 2. 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.

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**.
- **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.
-

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. 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.
4. Click **Save**.
5. If you are performing an initial Tenant setup, proceed to [Deploying the Agent to Your Endpoints](#) on page 34 to deploy the agent files to your endpoints.

6.5 Deploying the Agent to Your Endpoints

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
```

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.

7.0 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, refer 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 select the access permissions 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. (not available to Global Administrator) 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

- 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**.

8.0 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"> • EMALog-XXX.txt • 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. |