Intel® Endpoint Management Assistant (Intel® EMA)

Server Installation 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 **10**
1.1 Before you Begin 11
1.2 Supported Operating Systems 12
1.3 Installation Prerequisites 12
1.3.1 Computer 12
1.3.2 Operating System 12
1.3.3 Database 13
1.3.4 Pre-installation Instructions for Microsoft Azure AD Environments 15
1.3.5 Pre-installation Instructions for SAML Authentication Environments 16
1.3.6 Web Server 16
1.3.7 Intel® AMT PKI Certificate 17
1.3.8 Microsoft .NET Framework Versions 17
1.3.9 Firewall 17
1.3.10 Network 17
1.3.11 Network Ports 18
1.4 Security Recommendations 19
1.4.1 Perform a Backup of Important Data 19
1.4.2 Modify the Access Control List (ACL) for Key Configuration Files 20
1.4.3 Enable Transparent Data Encryption on SQL Server Enterprise 20
1.4.4 Secure all Certificates and Keys 20
1.4.5 Samples files for Intel® EMA REST API and JavaScript Library 20
1.4.6 Disable Insecure Cipher Suites 21
1.4.7 Strong Encryption Protocols 22
1.4.8 IIS – Replace the Temporary Web TLS Certificate 23
1.4.9 IIS – Change IIS User Account 23
1.4.10 IIS – Enabling the Transport Layer Security Protocol 24
1.4.11 IIS – Machine Key Validation Method 25
1.4.12 IIS – Restrict Unlisted IIS Extensions Execution 25
1.4.13 IIS – Dynamic IP Address Restrictions 25
1.4.14 IIS – Configure Host Headers for All Sites 25
1.4.15 IIS - Review updated web.config File 25
1.4.16 Check Binary Signatures 26
1.4.17 Change the Platform Manager Service User Account 26
1.4.18 Modify Permissions of SQL Server User, if Desired 28
1.4.19 User Creation and Management 28
1.4.20 Use SQL Server Installed with TLS 28
1.4.21 Set Custom Host Header Validations 28
1.5 Intel® EMA Installed Components 29
1.6 Important File and Directory Locations 31
1.7 Scaling Considerations 31

2.0 Installing or Updating the Intel® EMA Server **33**
2.1 Special Considerations for Installing All Components on One Machine 35
2.2 Installing Using the Setup Wizard 35
2.2.1 Initial Server Installation 36

2.2.2 Additional Server Installation....49
2.3 Performing an Update Installation Using the Setup Wizard....56
2.3.1 Load Balancer Information - Recovery Server....57
2.3.2 Server Components to Deploy....57
2.3.3 Platform Manager Configuration....57
2.3.4 Summary....58
2.4 Installing or Updating Using the Command Line....58
2.4.1 Initial Installation....59
2.4.2 Add an Additional Server....61
2.4.3 Performing an Update Installation Using the Command Line....64
2.4.4 Converting to Azure AD Using the Command Line....64
2.5 Uninstalling....65
2.5.1 Uninstalling Using the Installer GUI....65
2.5.2 Uninstalling Using the Command Line....66
2.6 Intel® EMA Installer Advanced Mode Menu Bar....67

3.0 Using the Global Administrator Interface....70
3.1 Changing the Global Administrator Password....70
3.2 Creating and Deleting Tenants....70
3.3 Managing Users and User Groups....71
3.3.1 Adding, Modifying, and Deleting Users....71
3.3.2 Creating New User Groups....71
3.3.3 Assigning Endpoint Groups to User Groups....71
3.3.4 Managing Active Directory User Groups....72
3.3.5 Managing SAML Authentication Users....72

4.0 Performing Intel® EMA Server Maintenance....74
4.1 Manually Installing Platform Manager....74
4.2 Configuring the Intel® EMA Platform Manager Service....74
4.2.1 Platform Manager TLS Certificate....74
4.2.2 Mutual TLS Certificate for Client Authentication....75
4.2.3 Kerberos with Active Directory in a Distributed Server Installation....75
4.3 Using the Intel® EMA Platform Manager Client Application....75
4.3.1 Starting Intel® EMA Platform Manager....75
4.3.2 The File Menu....77
4.3.3 Monitoring Component Server Events....77
4.3.4 Monitoring Component Server Internal Tracking Information....77
4.3.5 Performing Basic Controls on Component Servers....78
4.4 Deploying New Packages....81
4.5 Updating the Database Connection String....81
4.6 Revoking a Server's Certificate....82
4.7 Periodic Database Maintenance....83
4.8 Restoring the Intel® EMA Server from Backup....83

5.0 Appendix: Troubleshooting After Installation....86
5.1 General Troubleshooting....86
5.2 Distributed Server Installation Troubleshooting....91

6.0 Appendix - Modifying Component Server Settings....93
6.1 Swarm Server....93
6.2 Ajax Server....94
6.3 Manageability Server....95

6.4 Web Server....97
6.5 Security Settings....99
6.6 Recovery Server Settings....102

7.0 Appendix – Domain/Windows Authentication Setup....103

7.1 Server Connection Information Set at Installation....103
7.2 IIS Website's Authentication and .NET Authorization....103
7.3 Optional – Grant Permission to Website Content....103
7.4 Optional – Double-hop Structure....103
7.5 References....104

8.0 Appendix – Configuring 802.1X for Active Directory....105

8.1 Active Directory Domain Services....105
8.2 Active Directory Certificate Services....107

9.0 Appendix - Updating a Single Server Architecture Environment....109

9.1 Updating Using the Setup Wizard....110
9.1.1 Platform Manager Configuration....111
9.1.2 Summary....111
9.2 Updating Using the Command Line....111

Figures

1 URL Rewrite....29
2 Add New Organization Unit....106
3 Modify Security List of the Org Unit....107
4 Cert Authorization List....108
5 Certificate Templates list....108

Tables

1 Server Network Ports..... 18
2 Single Server Load.....32
3 Multi-Server Load..... 32

Revision History

Revision Number	Description	Release Date
1.14.0	Revision update only	August 2024
1.14.2	**Introduction** • Updated TCP protocol port number from 8083 to 8084 in Network Ports on page 18 • Updated point 3b in Pre-installation Instructions for Microsoft Azure AD Environments on page 15	February 2025
1.14.3	Revision update only	May 2025
1.14.4	**Introduction** • Added Pre-installation Instructions for SAML Authentication Environments on page 16 **Installing or Updating the Intel® EMA Server** • Added Note point 2 in Installing or Updating the Intel® EMA Server on page 33 • Added SAML Authentication on page 44 • Added Modify Server Settings for SAML Authentication on page 48 **Using the Global Administrator Interface** • Added Managing SAML Authentication Users on page 72 **Performing Intel® EMA Server Maintenance** • Added Note 3 and 4 in From the Intel® EMA Installer on page 75 • Added SAML to Note 11 in From Windows on page 76 • Added SAML to Load Solution in The File Menu on page 77 **Appendix: Troubleshooting After Installation** • Added Intel® EMA may fail to load and running Intel® EMA Agent in console mode details in General Troubleshooting on page 86 **Appendix - Modifying Component Server Settings** • Updated 2nd Table in Web Server on page 97	September 2025
1.14.5	Revision update only	February 2026
1.15.0	**Introduction** • Updated TCP Port 8080, 8081, and 8085 Usage in Table 1 on page 18 **Appendix: Troubleshooting After Installation** • Added Endpoints not connecting after update to Intel® EMA1.15.0 details in General Troubleshooting on page 86 table • Updated Distributed Server Installation Troubleshooting on page 91 table **Appendix - Modifying Component Server Settings** • Updated Manageability Server on page 95 table • Updated Web Server on page 97 table • Updated Security Settings on page 99 table	June 2026
1.15.1	**Supported Operating Systems**	October 2026

continued...

Revision Number	Description	Release Date
	• Added Microsoft Windows Server 2025 Note in Supported Operating Systems on page 12	

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.

1.1 Before you Begin

The actual installation of the Intel® EMA server and its components is fairly straightforward, as described in Installing or Updating the Intel® EMA Server on page 33. However, before starting the procedure, we recommend that you take time to consider the following choices so that you know in advance what to enter or select during the procedure.

- Ensure all prerequisites, described in Installation Prerequisites on page 12, are met.
- Review the Security Recommendations in Security Recommendations on page 19 and implement them as part of or after installing Intel® EMA.
- Review the Scaling Considerations in Scaling Considerations on page 31 to help you determine the right hardware to use for your Intel® EMA implementation.
- Determine the Fully Qualified Domain Name (FQDN) and/or IP Address that will be used to connect to the Intel® EMA server.
- For the SQL Server connection, decide if you want to use Windows authentication mode (recommended, for security reasons) or SQL Authentication. If SQL Authentication, you will need to ensure the target credentials are set up in SQL Server before installing.
- Determine how you will want the Intel® EMA website to be found via IIS and how it will process requests: by FQDN/hostname only; using FQDN/hostname first, then IP Address; by IP Address only. For additional hostnames to work correctly, and to manage them, you must configure a DNS server or a router.
- Decide which form of authentication you plan to install Intel® EMA under: Azure AD authentication, Windows AD domain authentication mode (Kerberos), or normal account (username/password) mode, which is the default. If you plan to use domain authentication, we suggest using the FQDN of your machine for the hostname. You still need to make sure 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 practice to set up the Service Principle Name (SPN) after Intel® EMA is installed.
- Determine the valid email address to use for the Global Administrator user.
- 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.

1.2 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

- Microsoft Windows Server 2025

  NOTE

  Crypto for Intel ME 11 systems is disabled by default on Windows Server 2025

1.3 Installation Prerequisites

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

1.3.1 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.

1.3.2 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).

1.3.3 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 enabling 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 to the Security Recommendations for information about changing these permissions and roles

1.3.4 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 anew 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" and "GroupMember.Read.All" permissions.
   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.

1.3.5 Pre-installation Instructions for SAML Authentication Environments

If you plan to install Intel® EMA in an existing SAML authentication environment, follow the steps below in order to enable Intel® EMA to successfully connect to the SAML 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 your SAML IdP (Identity Provider).

NOTE

Intel® EMA instances configured to use SAML 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 in 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 SAML authentication before proceeding with a production deployment.

1. Setup your SAML identity provider with the current Users, we will need two values, the SAML IDP Entity ID and the SAML IDP Metadata URL.
2. To configure SAML authentication, you will need the ACS (Assertion Consumer Service) URL: https://<EMA_URL>/saml/acs Replace <EMA_URL> with your EMA instance domain and enter this complete URL in your Identity Provider's SAML application settings as the Single Sign-On URL or ACS URL.

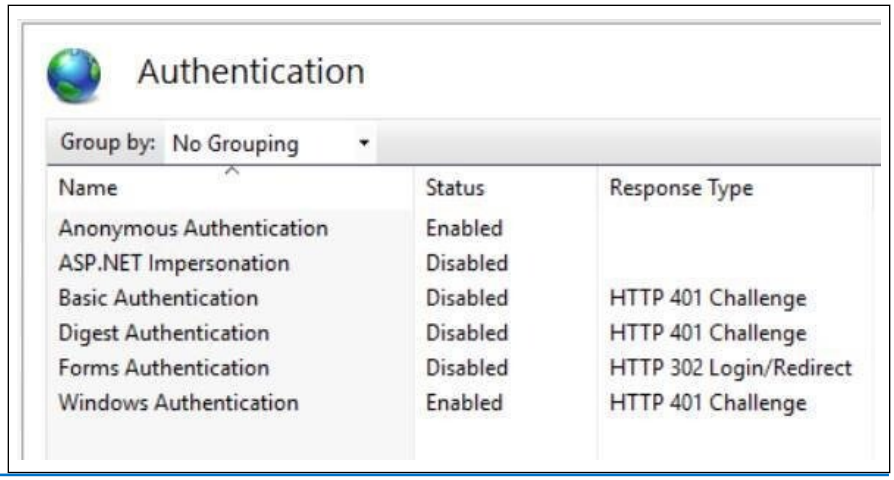
1.3.6 Web Server

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.



1.3.7 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.

1.3.8 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.

1.3.9 Firewall

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

1.3.10 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.

1.3.11 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. Uses 2048-bit keys.
TCP	8081	Agent, console, and Intel® AMT CIRA port. This is between client endpoints and the Intel® EMA Swarm server. Uses 3072-bit keys.
TCP	8084	Web redirection port. This is used between the web browser and the web server.

continued...

Protocol	Port	Usage
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 Appendix - Modifying Component Server Settings on page 93
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 Appendix - Modifying Component Server Settings on page 93
TCP	8092	The 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 Appendix - Modifying Component Server Settings on page 93
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 Appendix - Modifying Component Server Settings on page 93
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 Appendix - Modifying Component Server Settings on page 93
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. Refer Appendix - Modifying Component Server Settings on page 93
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.

1.4 Security Recommendations

This section details the security recommendations you should take into consideration when using Intel® EMA. Refer to industry best practices sources and your IT organization's policies for information on how to implement these recommendations.

1.4.1 Perform a Backup of Important Data

Intel® EMA's component servers rely on several certificates created during the Intel® EMA installation time.

The installer creates a self-signed MeshRoot root certificate, which it uses to create one or more MeshSettingsCertificates that are stored in the Local Machine\Personal certificate store. These MeshSettingsCertificate certificates are used to encrypt/decrypt the server settings stored in the database.

The MeshRoot certificate is used to create the mutual TLS certificates (EmaMtlsXXX) for the TCP-TLS communications between the Intel® EMA component servers (Ajax, Swarm, Manageability, Recovery, Web). They are stored in the Local Machine\Personal certificate store.

If these certificates are lost, there is no way to make Intel® EMA work again without completely reinstalling the Intel® EMA server.

Therefore, after installing the Intel® EMA server (or each server in a distributed environment), it is strongly recommended that you perform the following steps:

- Back up Intel® EMA database (this should also be done periodically, not just after setup).
- Back up the **MeshSettingsCertificate** which is stored in the Local Machine \Personal certificate store on your server machine. This certificate is used to encrypt/decrypt the server settings stored in the database.

1.4.2 Modify the Access Control List (ACL) for Key Configuration Files

After the Intel® EMA server installation, you should modify the ACL to limit access to the following files\folders:

- [Intel® EMA website root folder (e.g., C:\inetpub\wwwroot)] \ web.config.
- [Intel® EMA server installation folder (e.g., C:\Program Files (x86)\Intel\Platform Manager)] \ Platform Manager Server \ settings.txt
- [Intel® EMA server installation folder (e.g., C:\Program Files (x86)\Intel\Platform Manager)] \ Runtime \ MeshSettings \ connections.config
- [Intel® EMA server installation folder (e.g., C:\Program Files (x86)\Intel\Platform Manager)] \ Runtime \ MeshSettings \ app.config
- [Intel® EMA server installation folder (e.g., C:\Program Files (x86)\Intel\Platform Manager)] \ EMALogs

1.4.3 Enable Transparent Data Encryption on SQL Server Enterprise

To achieve security in-depth, we recommend that you use SQL Server Enterprise and enable Transparent Data Encryption.

1.4.4 Secure all Certificates and Keys

When Intel® EMA is installed, several certificates and encryption keys are generated. The certificates and encryption keys created by Intel® EMA expire after 20 years.

Certificates are stored in the Intel® EMA server database and in the server machine's certificate store. Take care to keep these certificates secure. If they are compromised, Intel® EMA cannot replace them and push them to the managed endpoints. In this case, you would need to uninstall and reinstall the Intel® EMA server using new certificates, then recreate all users and endpoint groups and then re-register all your endpoints.

Most of the encryption keys are stored in Intel® EMA server settings, which is encrypted and saved in the Intel® EMA server database.

1.4.5 Samples files for Intel® EMA REST API and JavaScript Library

The sample files are in the folder [Intel® EMA installation package folder] \Samples. These files are not automatically hosted on the Intel® EMA website during installation. These sample files are implemented using bare-minimum code to demonstrate how to use the API and do not use secure coding practices to guard against security concerns like cross-site scripting.

IMPORTANT

These samples should **never** be hosted in a production environment.

For hosting in a test environment for development purposes, copy the Samples folder to the Intel® EMA website root folder (e.g., C:\inetpub\wwwroot\).

1.4.6 Disable Insecure Cipher Suites

Cipher suites determine the key exchange, authentication, encryption, and algorithms used in an SSL/TLS session.

It is strongly recommended that you disable insecure cipher suites to restrict the use of weak cryptographic algorithms and protocols for TLS connections.

By default, many versions of Microsoft Windows Server may have an insecure cipher suite configuration. The following are the warnings or threats that result from insecure ciphers:

- 64-bit block cipher 3DES vulnerable to SWEEET32 attack
- Broken cipher RC4 is deprecated by RFC 7465
- CBC-mode cipher in SSLv3 (CVE-2014-3566) – Oracle padding
- Cipher suite uses MD5 for message integrity
- Weak certificate signature for SHA1
- Key exchange (DH 1024) is of lower strength than the certificate key

One workaround to avoid these threats and warnings is to download IIScrypto from this website: https://www.nartac.com/Products/IIScrypto. This product helps to change schannels and cipher settings.

You must run the IIScrypto program and de-select the multi-protocols: unified hello, PCT 1.0, SSL2.0, MD5, and all ciphers above triple DES. This helps clear all the aforementioned warnings (except for the SHA1 warning).

IMPORTANT

Intel® EMA and Intel AMT require one of the following Cipher Suites to be enabled in order to effectively communicate and function. As an example, enabling "TLS_RSA_WITH_AES_128_GCM_SHA256" would work for all versions of Intel AMT currently supported by Intel® EMA.

Intel AMT version 11.8:

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

Intel AMT version 12:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

Intel AMT versions 14 and 15:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

Intel AMT version 16:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_AES_128_GCM_SHA256

1.4.7 Strong Encryption Protocols

We strongly recommend that you disable weak encryption protocols, such as PCT 1.0, SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1, and instead enable strong encryption protocols, such as TLS 1.2 and TLS 1.3. Additionally, we recommend that you use the Diffie-Hellman Ephemeral (DHE) protocol.

NOTE

Intel® EMA will not support Intel AMT versions below 11.8.77.3664, as those versions use TLS 1.1 which is no longer supported in Intel® EMA.

1.4.8 IIS – Replace the Temporary Web TLS Certificate

The Web TLS certificate is used for HTTPS communications between the Web browser and the Web + AJAX Server. A temporary self-signed Web TLS certificate is created during installation. This certificate can be replaced at any time. We recommend that you use a valid HTTPS certificate issued from a valid trusted Certificate Authority.

NOTE

This TLS certificate can also be used for the Platform Manager TLS certificate if you are running Platform Manager on the same system as the IIS server. Refer Configuring the Intel® EMA Platform Manager Service on page 74.

For the self-signed website TLS certificate (and the Intel® EMA settings certificate), Intel® EMA grants the default IIS DefaultAppPool account read access to the private key. If you change the account that the IIS default application pool will run under, you must also change the access control accordingly.

To replace the temp Web TLS Certificate:

1. Install the new certificate in the Local Machine\Personal certificate store.
2. Run the IIS Manager on the Web Server (IIS Server).
3. Place the certificate in the Server Certificates.
4. Edit the Bindings section in the Default Website dialog box to use the new certificate.

1.4.9 IIS – Change IIS User Account

By default, Intel® EMA uses the IIS default application pool (app pool) to run the Intel® EMA website. This default app pool uses the ApplicationPoolIdentity account by default. In a distributed installation running under Windows authentication, where the Intel® EMA component servers need to access a remote SQL Server, you may need to change the account the Intel® EMA website runs under to one that can access the remote SQL Server.

To do this, follow the steps below:

1. Give the account access to Intel® EMA assets (files and folders, certificate's private key).
   a. Skip these steps if the account already has the necessary privileges.
   b. If the SQL connection is using Windows authentication, ensure the new IIS user account satisfies the permission and role requirements for the SQL Server account. Refer Modify Permissions of SQL Server User, if Desired on page 28.
   c. Change the service to run under the desired account.
   d. Give read and write access to **[System drive]\Program Files (x86)\Intel\Platform Manager\EMALogs**.

e. Give full control to the following:
   - [System drive]\inetpub\wwwroot: also for all sub-folders and files.
   - [System drive]\inetpub\wwwroot\web.config
   - [System drive]\Program Files (x86)\Intel\Platform Manager\Runtime \MeshSettings\app.config
   - [System drive]\Program Files (x86)\Intel\Platform Manager\Runtime \MeshSettings\connections.config
   - [System drive]\ProgramData\Intel\EMA\USBR - Or the USBR image path if you have updated it as described in Manageability Server on page 95

f. Use the Windows certlm tool to open the certificate store for Local Computer \Personal\Certificates and give "read" permission for the following certificates by right-clicking the target certificate and selecting All Tasks\Manage Private Keys:
   - Temporary Web TLS certificate. "Issued To" is the Intel® EMA web site FQDN or IP. "Issued By" is "MeshRoot-XXXX".
   - Settings certificate. "Issued To" is "MeshSettingsCertificates-XXX". "Issued By" is "MeshRoot-XXXX".
   - Inter-component TLS certificate for web server. "Issued To" is "EmaMtlsWeb-XXX". "Issued By" is "MeshRoot-XXXX".

2. Add a new IIS application pool for Intel® EMA.
   a. Use IIS Manager to create a new app pool.
   b. Choose **.NET CLR Version v4.0.XXX, Integrated** pipeline mode, and **Start app pool immediately**.
3. Assign an account to the new application pool.
   a. Use IIS Manager to change the account for the new app pool.
   b. Choose **Custom Account** and specify the desired Windows account.
4. Use IIS Manager to change the application pool used by Intel® EMA to the new one created above. Then restart the whole web site. For verification, access the Intel® EMA web site in a browser, then use Windows Task Manager to verfiy that the **w3wp.exe** process is running under the specified account.

1.4.10 IIS – Enabling the Transport Layer Security Protocol

It is strongly recommended that you enable Transport Layer Security (TLS), which is an industry-standard protocol designed to protect the privacy of information communicated over the internet.

The TLS protocol enables clients/server applications to detect these security risks:

- Message tampering
- Message interception
- Message forgery

HTTP Strict Transport Security (HSTS) is an opt-in security enhancement policy, which must be enabled to ensure connections can only be successful if the Transport Layer Security (TLS) protocol is used.

1.4.11 IIS – Machine Key Validation Method

The machine key element in the ASP.NET web.config specifies the algorithm and keys to be used by an application for encryption and hashing. Ensure that one of the SHA-2 family methods (for example, HMACSHA256) is configured as the validation method for the machine key

1.4.12 IIS – Restrict Unlisted IIS Extensions Execution

If IIS features ISAPI Extensions or CGI are installed, ensure that unspecified ISAPI modules or unspecified CGI modules, respectively, are not allowed to run.

1.4.13 IIS – Dynamic IP Address Restrictions

Dynamic IP Address Restrictions is an IIS setting that can be used to mitigate against DDoS and brute force attacks. For single server installations, in IIS Manager, enable "Deny IP Address based on the number of concurrent requests", enable "Deny IP Address based on the number of requests over a period of time", and then set values required to protect your environment.

For more information, refer the following link:

https://docs.microsoft.com/en-us/iis/manage/configuring-security/using-dynamic-ip-restrictions

1.4.14 IIS – Configure Host Headers for All Sites

If multiple websites will be hosted in IIS on the same IP address and port, configure host headers for all sites.

1.4.15 IIS - Review updated web.config File

The Intel® EMA server installation adds the following headers to your **web.config** file, and renames the existing web.config file to **web.config.original.<date>**. After installation, review the new web.config file and modify if desired.

For more information about HTTP headers, refer to the following link:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers

The following headers are automatically added to the **web.config** file during installation.

Header	Value
X-Content-Type-Options	`nosniff`
X-XSS-Protection	`1; mode=block`
X-Frame-Options	`SAMEORIGIN`

continued...

Header	Value
Referrer-Policy	`strict-origin`
Expect-CT	`max-age=86400, enforce`
Feature-Policy	`payment 'none'; microphone 'none'; geolocation 'none';`
strict-transport-security *Note:* Added by IIS rewriter rule	`max-age=31536000; includeSubDomains;`
Content Security Policy (CSP) *Note:* Added by plugin	`default-src 'self' blob:;script-src 'self' 'unsafe-inline' 'nonce-<autogen_value> ' 'sha256-<multiple values> ';object-src 'none';style-src 'self' 'unsafe-inline' https://fonts.googleapis.com;img-src 'self' data:;font-src 'self' data: https://fonts.gstatic.com;base-uri 'none';worker-src 'self' blob:`

The CORS header is added but commented out by default. To enable it, edit the web.config file and remove the comment tags and add your domain information.

```
<!---
<add name="Access-Control-Allow-Origin" value="https://<YOURDOMAINHERE>" />
<add name="Access-Control-Allow-Headers" value="Content-Type" />
<add name="Access-Control-Allow-Methods" value="GET,POST,PUT,DELETE,OPTIONS" />
-->
```

Lastly, the **X-Robots-Tag** header is added, which disables web search engines from finding installed instances of the Intel® EMA server.

NOTE

Intel® EMA grants the default IIS DefaultAppPool account read access to the web.config file. If you change the account that the IIS default application pool will run under, you must also change the access control accordingly.

1.4.16 Check Binary Signatures

All Intel® EMA binaries are signed as an integrity mechanism. We recommend that you check and confirm the signatures on these files. Further, we recommend that you only use installation packages from trusted sources (such as www.intel.com).

1.4.17 Change the Platform Manager Service User Account

Perform this action after installing the Intel® EMA server. By default, the Intel® EMA Platform Manager service runs under the System user. To improve security, we recommend that you modify this service to run as a local or domain user.

NOTE

Whatever account you set Platform Manager to run under will be the account that all Intel® EMA component server services (i.e., Manageability Server, Swarm Server, etc.) run under as well. After the Platform Manager account is changed, the component server services will use the new account once they are restarted. In a distributed server environment this must be done for each Platform Manager instance.

The account that Platform Manager runs under needs to have correct permissions to perform deployment and management of IIS websites. For further information, refer https://learn.microsoft.com/en-us/troubleshoot/developer/webapps/iis/www-authentication-authorization/default-permissions-user-rights.

First, give the account access to Intel® EMA assets (files and folders, certificate's private key).

1. Skip these steps if the account already has the necessary privileges.
2. If the SQL connection is using Windows authentication, ensure the new user account satisfies the permission and role requirements for the SQL Server account. Refer section below.
3. Change the service to run under the desired account.
4. Give read and write access to **[System drive]\Program Files (x86)\Intel\Platform Manager\EMALogs.**
5. Give full control to the following:
   - **[System drive]\inetpub\wwwroot**: also for all sub-folders and files.
   - **[System drive]\inetpub\wwwroot\web.config**
   - **[System drive]\Program Files (x86)\Intel\Platform Manager**
   - **[System drive]\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\app.config**
   - **[System drive]\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config**
   - **[System drive]\ProgramData\Intel\EMA\USBR** - Or the USBR image path if you have updated it as described in Manageability Server on page 95.
6. Use the Windows certlm tool to open the certificate store for Local Computer \Personal\Certificates and give "read" permission for the following certificates by right-clicking the target certificate and selecting All Tasks\Manage Private Keys:
   - Temporary Web TLS certificate. "Issued To" is the Intel® EMA web site FQDN or IP. "Issued By" is "MeshRoot-XXXX".
   - Recovery certificate. "Issued To" is the Intel® EMA web site FQDN or IP. "Issued By" is "MeshRoot-XXXX".
   - Settings certificate. "Issued To" is "MeshSettingsCertificates-XXX". "Issued By" is "MeshRoot-XXXX".
   - Inter-component TLS certificate for web server. "Issued To" is "EmaMtlsWeb-XXX". "Issued By" is "MeshRoot-XXXX".
   - Note that the Temporary Web TLS certificate and the Recovery certificate look similar in the listing, but if you open them and go to the Details tab, you can see which is which.

Next, ensure the file **settings.txt** in the Intel® EMA installation folder has read/write permissions for the new Platform Manager service account.

Lastly, find **Intel Platform Manager** in **Windows services** and change the user account under which this service is running, then restart all the Intel® EMA component servers.

1.4.18 Modify Permissions of SQL Server User, if Desired

NOTE

Two database accounts are required when using SQL authentication: one of the installer which requires DB Owner permissions, and one for the Intel® EMA services, which allows the database service to be run with lesser privileges.

The first account, for the installer, needs db_owner, db_datawriter, and db_datareader permissions to create the Intel® EMA database during installation. These permissions are granted by default during Intel® EMA installation.

The second account you specify during installation requires Execute permission to run all Intel® EMA stored procedures.

Also, you must grant permission for "SUBSCRIBE QUERY NOTIFICATIONS" to the user of Intel® EMA database.

1.4.19 User Creation and Management

It is strongly recommended that you periodically check existing user accounts for Intel® EMA and ensure that any accounts that are no longer being used are deleted. See the Intel® EMA Administration and Usage Guide for information on creating, modifying, and deleting user accounts.

1.4.20 Use SQL Server Installed with TLS

It is strongly recommended that you use an instance of SQL Server that has been installed with TLS to encrypt data transmitted between SQL Server and Intel® EMA. For more information, see the link below:

https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15

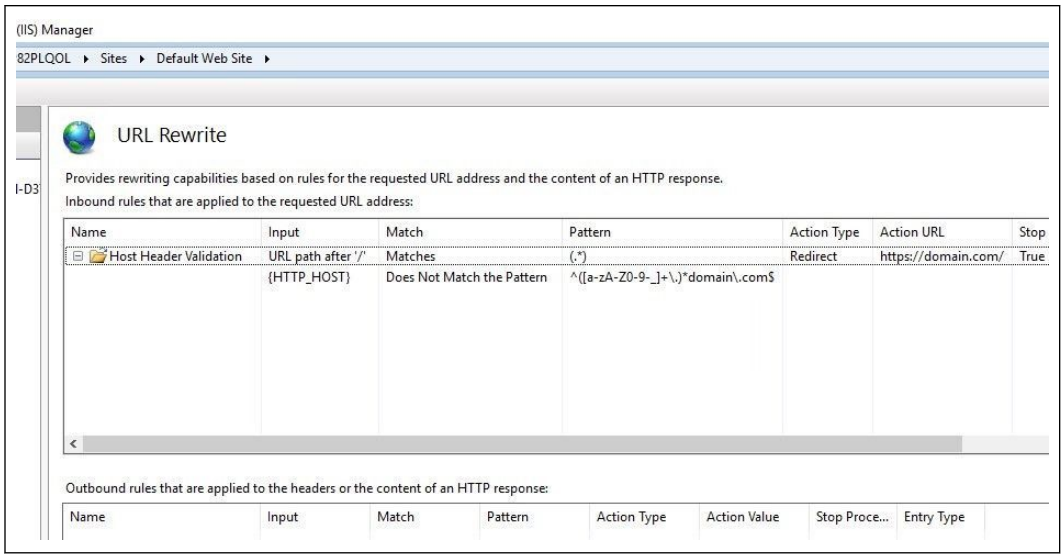
1.4.21 Set Custom Host Header Validations

URL Rewrite rules can be used to find malicious host headers:

1. Click on the site in IIS Manager
2. Go to **URL Rewrite** (This must be installed initially. Refer https://www.iis.net/downloads/microsoft/url-rewrite)
3. Click **Add Rule(s)**
4. Select **Blank rule**
5. For **Match URL** section, enter (.) into the **Pattern**

6. In **Conditions** section, click **Add**
7. Enter **{HTTP_HOST}** into **Condition** input
8. Select **Does Not Match the Pattern** from **Check if input string** list
9. Enter **^([a-zA-Z0-9-_]+.)*domain.com$** into **Pattern** field (change domain name with yours)
10. For the **Action** section, select **Redirect** from the **Action type** list
11. Enter your domain address (https://domain.com/) in the **Redirect URL**
12. Select **Permanent (301)** from the **Redirect type** list
13. Click **Apply**

Figure 1. URL Rewrite



1.5 Intel® EMA Installed Components

After installation, most software components are installed in the **C:\Program Files (x86)\Intel\Platform Manager** folder. The main components are as follows:

- Intel® EMA Platform Manager service:
  - Installed as an auto-started Windows service with display name **Intel® EMA Platform Manager** and service name **PlatformManager**
  - Deploys the Intel® EMA website content to the IIS server
  - Monitors Intel® EMA component servers on the machine and auto-starts any that are not running
  - In a distributed server architecture, each Intel® EMA server machine will have its own Platform Manager service
- Intel® EMA Platform Manager client application:
  - Installed as a Windows desktop application
  - Provides the graphical user interface (GUI) for user interaction

  - Used for checking Intel® EMA internal server events and performing simple server controls
  - Can communicates with the Platform Manager service on a local or remote machine
  - Can communicates with the Platform Manager service on a local or remote machine
- Intel® EMA website:
  - Primary GUI for end users
  - Deployed on the IIS server by the Platform Manager service after installation
  - May have multiple instances in a distributed environment
  - Refer Intel® EMA Administration and Usage Guide for further details
- Intel® EMA REST APIs:
  - Deployed on the IIS server by the Platform Manager service after installation
  - Enables third-party software development to create a different Intel® EMA GUI for end users
  - Refer Intel® EMA APi Guide for further details
- Intel® EMA JavaScript libraries:
  - Deployed on the IIS server by the Platform Manager service after installation
  - Delivers some features that REST APIs are not designed to support
  - Enables third-party software development to create a different Intel® EMA GUI for end users
  - Refer Intel® EMA JavaScript Libraries Guide for further details
- Intel® EMA AJAX server:
  - Started by the Platform Manager service
  - Handles the JavaScript library's requests
  - May have multiple instances in a distributed environment
  - Refer Intel® EMA Administration and Usage Guide for further details about the scheduled tasks feature
- Intel® EMA Swarm server:
  - Started by the Platform Manager service
  - Accepts the TCP connection from the endpoints (devices) and handles communication between endpoints
  - May have multiple instances in a distributed environment
- Intel® EMA Manageability server:
  - Started by the Platform Manager service
  - Manages Intel AMT provisioning and unprovisioning requests for endpoints
  - Talks to the Swarm server to send provision/unprovision requests to the endpoints
  - Only one instance in a distributed environment
- Intel® EMA Recovery Server:
  - Started by the Platform Manager service

  - Used for initiating recovery process to return specified endpoint's OS to a last known good state in a secure manner
  - May have multiple instances in a distributed environment
- Intel® EMA Agent:
  - Agent software is not installed on the server machine
  - Agent installer is included in Intel® EMA software package
  - Agent must be installed on the endpoint for the Intel® EMA server to manage it
  - Refer Intel® EMA Administration and Usage Guide how to download and manage the agent installers

1.6 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 • 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.

1.7 Scaling Considerations

As you plan your Intel® EMA server implementation, keep in mind that the configuration of the server hardware can have an impact on the overall performance of your Intel® EMA instance as the number of managed endpoints grows. The following tables show testing results that may be helpful in determining the appropriate server hardware configuration for your Intel® EMA server installation. The tables show the number of managed endpoints required to achieve maximum capacity in the DB (DB 100% CPU) then next to it shows the average CPU capacity on Intel® EMA servers when it hit max load on DB given the server and database hardware configurations in the row labels (e.g., 4 CPUs and 16 GB memory).

NOTE

Performance can vary greatly from one implementation to another depending on a variety of environmental factors. The following test result information is provided solely to aid in pre-implementation decision making and is not intended as any claim of actual performance.

Based on the following test result data, for example, you could expect a single Intel® EMA server with 2 CPUs and 8 GB of RAM to satisfactorily support approximately 79K managed endpoints (the DB 80% CPU column below). Note that if CIRA will be used, we recommend that you reduce the number of endpoints in any column below by half.

Furthermore, the data below is based on an idle state for the Intel® EMA agent on the managed endpoint. You should allow some headroom (for example, 20%) for usage such as KVM sessions on the endpoint.

Given the above considerations, for a single Intel® EMA server with 2 CPUs and 8 GB of RAM and using a database with 4 CPUs and 16 GB of RAM in an implementation where CIRA will be used, we recommend no more than approximately 31K managed endpoints (79K/2 * .80 = 31.6). Note also that in a multi-server configuration, adding additional servers does not necessarily increase linearly the number of managed endpoints as there is an overload on the database.

Table 2. Single Server Load

Intel® EMA Server Configuration	Intel® EMA % CPU	DB 80% CPU	Intel® EMA % CPU	DB 100% CPU	DB Configuration
2 CPU, 8 GB memory	~50%	~79K	~65%	~96K	4 CPU, 16 GIG Memory
8 CPU, 32 GB memory	~24%	~80K	~30%	~100K	8 CPU, 32 GIG Memory

Table 3. Multi-Server Load

Number of Intel® EMA Servers (8 CPU, 32 GB memory	Intel® EMA % CPU	DB 80% CPU	Intel® EMA % CPU	DB 100% CPU	DB Configuration
2	~24%	~160K	~30K	~200K	8 CPU, 32GB Memory
3	~24%	~240K	~30K	~300K	8 CPU, 32GB Memory
4	~20%	~276K	~25%	~345K	8 CPU, 32GB Memory

2.0 Installing or Updating the Intel® EMA Server

Follow the steps below to install the Intel® EMA server. For updating, refer Performing an Update Installation Using the Command Line on page 64.

NOTES

- If you plan to use Azure AD authentication, you must follow the pre-installation steps in Azure AD as described in Pre-installation Instructions for Microsoft Azure AD Environments on page 15.
- If you plan to use SAML authentication, you must follow the pre-installation steps in SAML Authentication as described in Pre-installation Instructions for SAML Authentication Environments on page 16
- Do not edit the Intel® EMA database to manually add a user to the user table. Use the Intel® EMA user interface (either GUI or API) to create all Intel® EMA user accounts.
- Installing two separate Intel® EMA instances that use the same Intel® EMA database is not supported. Note that this is different from a distributed server architecture installation in which an Intel® EMA instance's server components are installed on multiple machines.
- Having multiple instances of the Manageability Server component server running is not supported. However, installing a second instance of the Manageability Server for failover purposes is allowed as long as the Manageability service on the second instance is stopped and disabled. If there are no active Manageability Servers, you will still be able to manage existing endpoints but you will not be able to provision new endpoints or utilize the USB Redirection (USBR) feature. If needed, in a failover scenario, this second instance can be started. When started, the Intel® EMA component server settings must be updated to point to the IP address of new Manageability Server. Refer Appendix - Modifying Component Server Settings on page 93 for information on modifying component server settings.
- If you are using a remote SQL database, and you do not plan to change the account under which Platform Manager and the Intel® EMA component servers run (Note, it is recommended to change this account, per Security Recommendations on page 19), then before installing Intel® EMA you must manually create an account on the remote SQL database for the system account of the machine on which the Intel® EMA server will be installed.
- 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. To enable these features, the installer creates a folder that is accessible to the accounts under which all Intel® EMA Web Server components, all Recovery Server components, and the Manageability Server component are running. This folder will be used by Intel® EMA to store uploaded image files and to access those stored image files when mounting an image file to a managed endpoint.
- 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.

2.1 Special Considerations for Installing All Components on One Machine

Intel® EMA allows you to install all server components of the distributed server architecture (i.e., Swarm Server, Ajax Server, etc.) on the same machine (or virtual machine), if desired.

NOTE

This is still a distributed server architecture installation, not a single server architecture.

The installation process is essentially the same as installing the various components on separate machines. However, there is one crucial difference with regard to the load balancer that is required when installing components on separate machines.

When you install all components on the same machine, you do not need an actual load balancer. Therefore, during installation, when asked to configure a load balancer, simply enter the IP Address or FQDN of the system on which you are installing all Intel® EMA server components.

IMPORTANT

If you plan to expand your Intel® EMA server implementation to be truly distributed across multiple machines or VMs in the future, you will need to configure an actual load balancer at that time. When you do so, you MUST rename (FQDN) the machine on which you originally installed Intel® EMA, and then name (FQDN) the load balancer machine exactly what the original Intel® EMA server machine was named.

This is because during installation, Intel® EMA configures several certificates that govern communication between the server components. The load balancer FQDN (or IP Address) is associated with these certificates, and CANNOT be changed after installation. Therefore, if you configure a real load balancer at a later time after installing all components on one machine, the load balancer FQDN MUST match the name associated with the certificates.

This also applies to the IP Address of the original Intel® EMA server machine and the load balancer; the original server machine must be given a new IP Address, and the load balancer given the previous IP Address of the original server machine, so that the load balancer's IP Address matches the certificates.

Lastly, when installing all components on the same machine or VM, you do not need to perform the steps in the install wizard for installing additional servers.

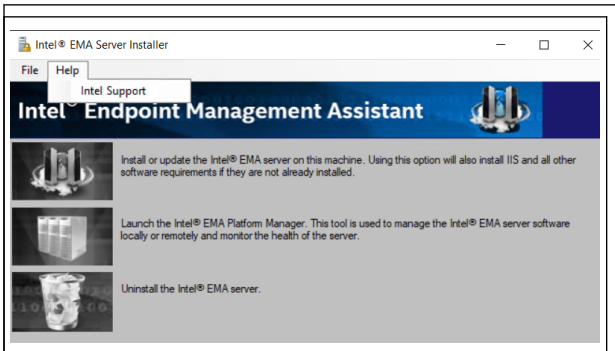
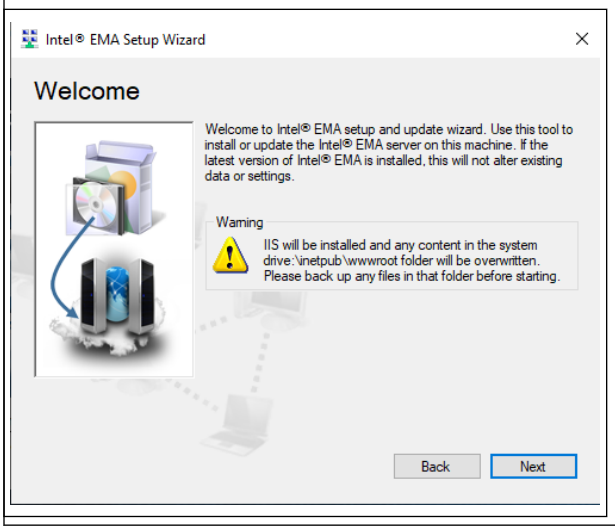
2.2 Installing Using the Setup Wizard

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

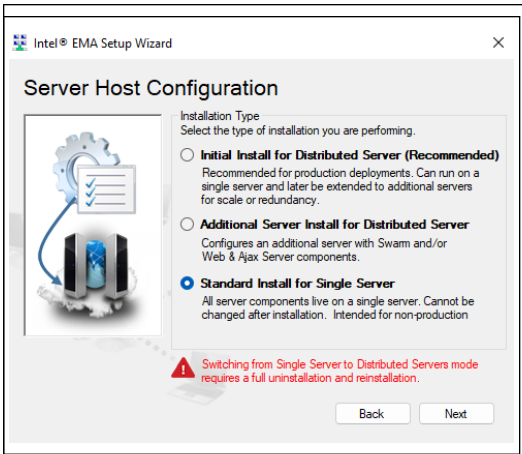
2.2.1 Initial Server Installation

NOTE

Be sure to read all notes at the start of Installing or Updating the Intel® EMA Server on page 33 before performing the steps in this section.

	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.

2.2.1.1 Server Host Configuration



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

Note: **Initial Install for Distributed Server Architecture** is the recommended choice for first time installations because it is expandable if you want to add more server machines to the Intel® EMA server instance in the future. Switching from Single Server to Distributed Servers requires a full uninstallation and reinstallation. For Distributed Server installation instructions, refer the Intel® EMA Distributed Server Installation and Maintenance Guide.

Choose which installation type you want to perform. Do not choose Standard Install for Single Server Architecture if performing a distributed installation

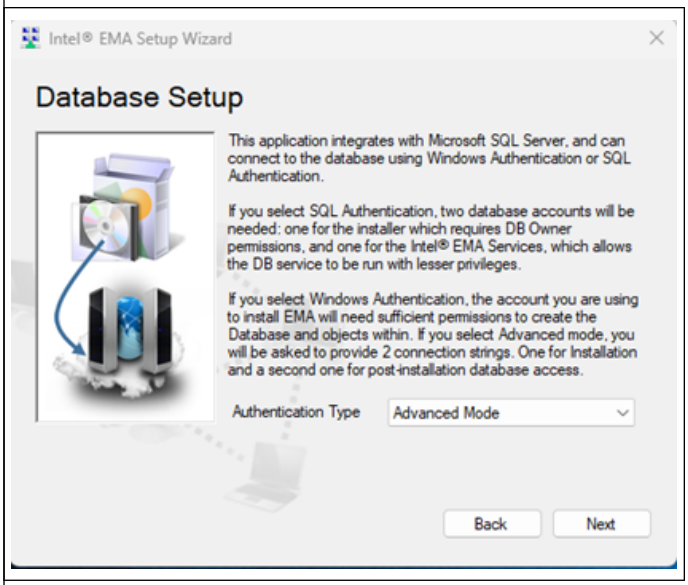
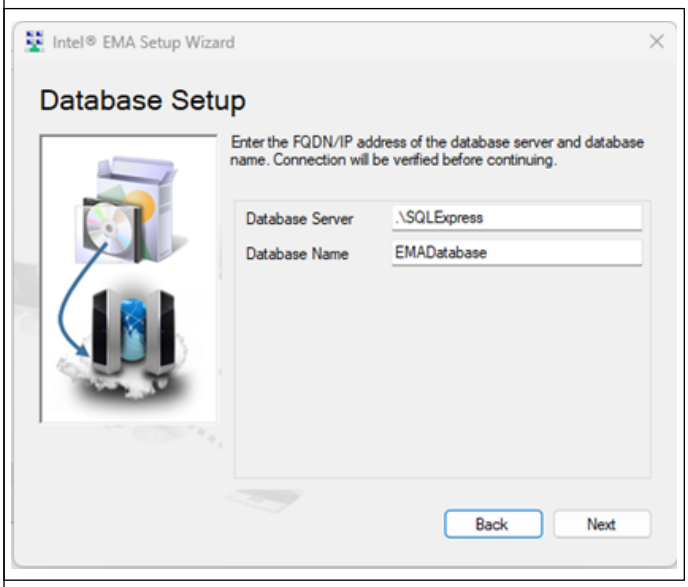
This process also lets you specify a configured load balancer to manage the workload between the multiple server machines.

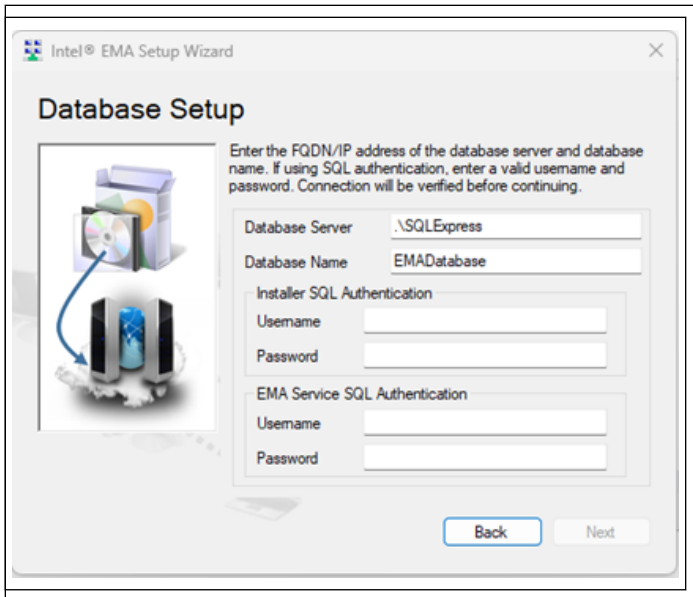
Additional Server Install for Distributed Server Architecture

Use this option AFTER completing the Initial Install for Distributed Architecture option above. This option allows you to install additional server components on a different server machine than the initial distributed installation.

Skip to Additional Server Installation on page 49

2.2.1.2 Database Settings

	Select the desired authentication type: Windows Authentication, SQL Authentication, or Advanced Mode. *Note:* 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.
	If you choose Windows Authentication the account you are using for installation will be used to authenticate against the SQL server and create the database. 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. 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.



If you choose 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.

Note: 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.

The connection string is encrypted and stored in **c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config**.

Important: If installing a distributed server architecture, copy the customized connection strings to a text file to save it for use when installing additional servers.

Note: During an upgrade, the connection information is displayed but cannot be edited as part of the installation flow. Refer Updating the Database Connection String on page 81for information on editing connection strings.

2.2.1.3 Load Balancer Information

For Identity mode:

- **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

Note: 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.

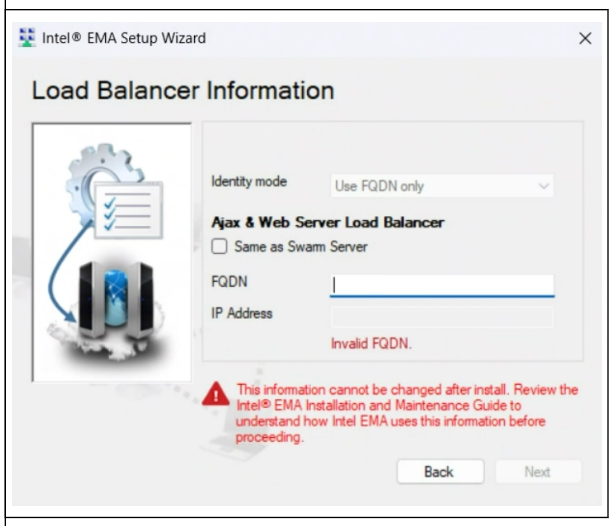
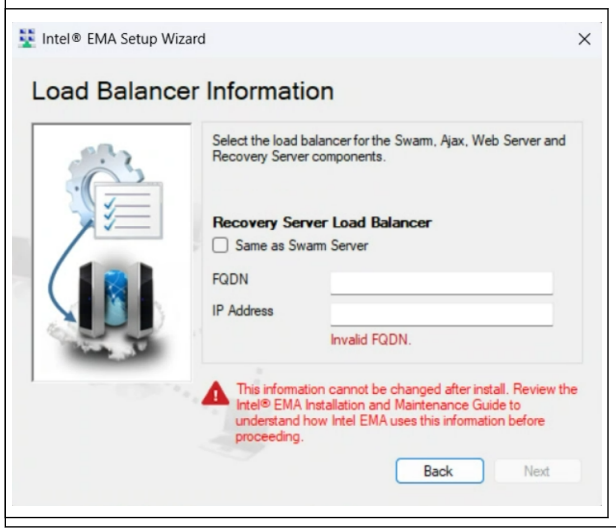
Intel AMT relies on DNS lookups to resolve remote hosts. If you choose to use a short name/host name for your server instead of a DNS resolvable FQDN, Intel AMT remote management functionality may not work correctly.

Enter the **FQDN** and/or **IP Address** (or both, depending on Identity mode) of the load balancer for the Swarm Server.

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.

Refer *Special Considerations for Installing All Components on One Machine* for special considerations in this case.

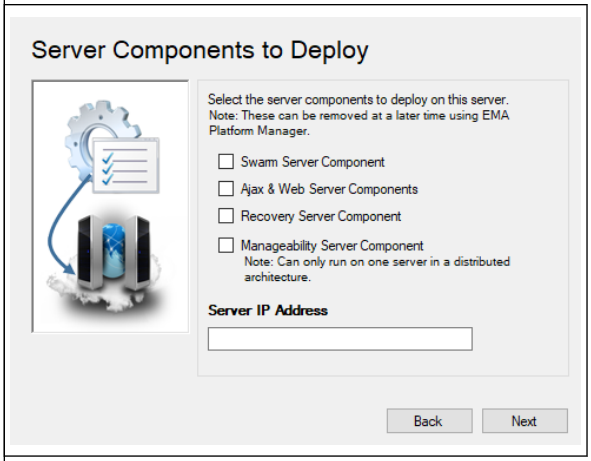
continued...

	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**).
	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**).

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).

2.2.1.4 Server Components to Deploy

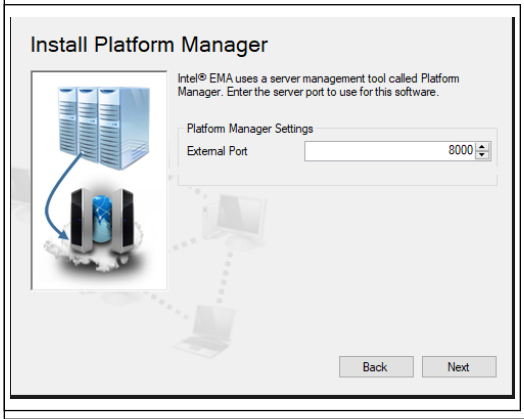


Specify which server components to deploy on this server machine, then verify the **IP Address** of this server machine (field filled in by default).

Note: Only one machine can run the Manageability Server component.

For information about the various server components, refer *Intel® EMA Installed Component*.

2.2.1.5 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.

2.2.1.6 User Authentication

Choose which form of authentication you wish to use.

2.2.1.6.1 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.

2.2.1.6.2 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).

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. See the following link for more information: https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts.

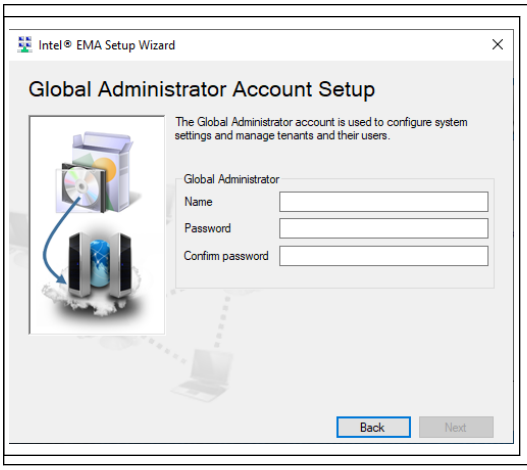
2.2.1.6.3 Azure Active Directory Authentication

If your IT enviroment 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.

2.2.1.6.4 SAML Authentication

If your IT environment wants to use SAML SSO authentication, you have the option to select SAML authentication. This option allows you to enter the username and password for the first account with Global administrator role. This account doesn't need to be setup on your identity provider. After installation, you can use this account to log in and create subsequent users, which must be configured in your SAML identity provider configuration page.

2.2.1.7 Global Administrator Account Setup

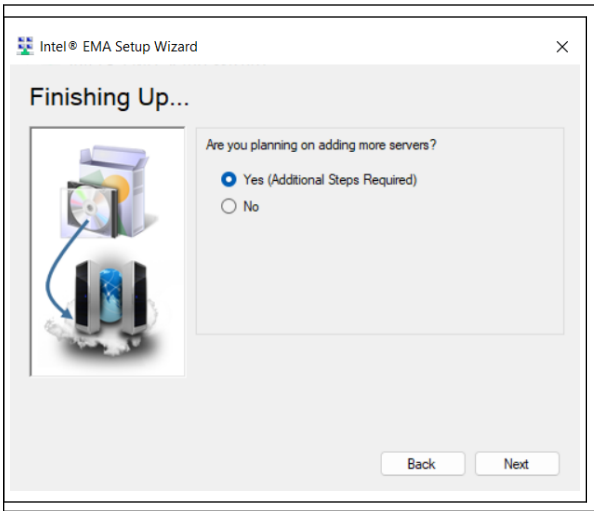


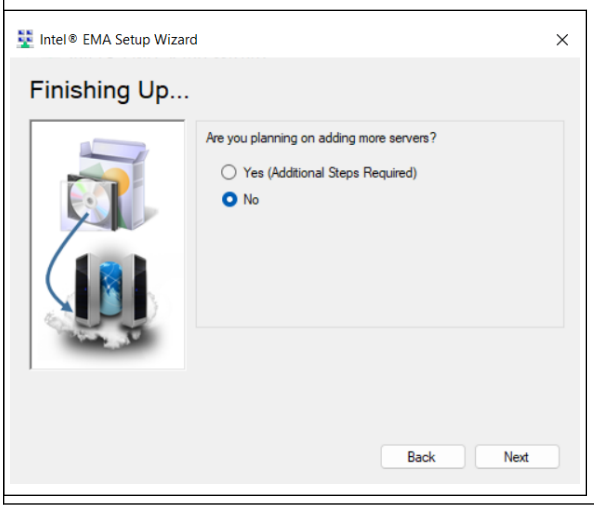
This screen only appears during setup if you have chosen "Normal accounts" or "Azure AD Authentication" for user authentication. If using domain accounts, the user running the installer will be made a Global Administrator.

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 47

2.2.1.8 Finishing Up



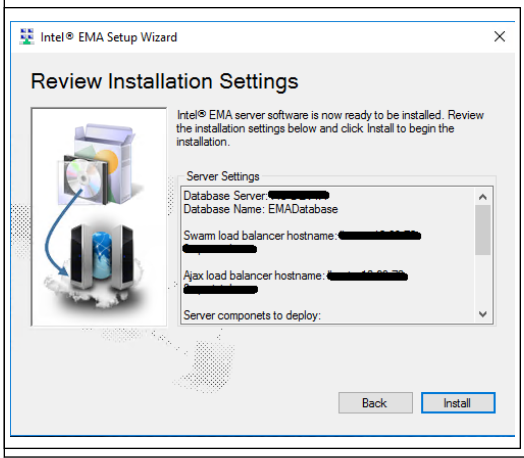


If you are planning to add more servers to this Intel® EMA installation, choose Yes. Proceed to the Summary screen, then once the installation completes successfully, perform the steps in sections Create Shared Folder on page 46 and Modify IIS Settings If Ajax and Web Server Components Installed on page 47.

If you do not plan to install more servers at this time, choose No. The installer will automatically create a folder required for the USBR feature (see the for more information on this feature).

You do not need to perform the steps in sections 2 and 3 if you choose No on this screen.

2.2.1.9 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.

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 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.
```

If you are only installing one server at this time, you are now ready to log in as the Global Administrator and click View Getting Started tips under Getting Started on the overview page. Refer Using the Global Administrator Interface. Otherwise, proceed to section below.

2.2.1.10 Create Shared Folder

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. To enable this feature, you must create a shared folder that is accessible to the accounts under which all Intel® EMA Web Server components and the Manageability Server component are running. This folder will be used by Intel® EMA to store uploaded image files and to access those stored image files when mounting an image file to a managed endpoint.

NOTES

- This procedure is not required on additional servers in a distributed server installation.
- This procedure is not required if you installing only one server at this time.

Follow the steps below.

1. Create a folder on the initial Intel® EMA server or a location that will be accessible to all Intel® EMA servers in the distributed server installation.
2. Set **Sharing** for the folder so that the accounts under which the Intel® EMA Web Server component (on all servers in the distributed installation), the Recovery Server, and the Intel® EMA Manageability Server component are running can access this shared folder. The account for the Web Server (IIS) needs read/write access. The account for the Manageability Server needs read access. Sharing can be set by right-clicking the folder name in Windows Explorer, selecting **Properties**, then selecting the **Sharing** tab.
3. Launch the Intel® EMA web-based UI and log in as the Global Administrator (Refer Using the Global Administrator Interface).
4. From the navigation panel at left, select **Settings** and then select the **Server Settings** tab.
5. For the Manageability Server, set the **USBR Images Root Directory** setting to the shared folder you just created (for example, `\\myserver.domain.com\sharename`). For more information about Server Settings, referAppendix - Modifying Component Server Settings on page 93.

2.2.1.11 Modify IIS Settings If Ajax and Web Server Components Installed

NOTE

This procedure is not required if you installing only one server at this time.

If you selected the **Ajax and Web Server components** on the **Server Components to Deploy** screen above, you need to modify your IIS settings to set up fixed machine keys. This will allow other Web Servers to use the same keys if you install additional server components on other virtual or physical machines.

1. In IIS Manager, stop the Default Web Site.
2. In IIS Manager, open your server in the left-hand pane and double-click the **Machine Key** section under ASP.NET and set the **Encryption method** to AES and the **Validation method** to one of the SHA-2 family methods (for example, HMACSHA256).
3. Under Actions at right, click **Generate Keys** to generate the **Validation key** and the **Decryption key**. You will need these keys later when you install additional servers (Refer Using the Global Administrator Interface).
4. Click **Apply** and then restart the Default Web Site.

If you are installing in Azure AD authentication mode, proceed to section Modify Server Settings for Azure AD. Otherwise, you are ready to install additional Intel® EMA servers, as described in Section Additional Server Installation on page 49

2.2.1.12 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. Refer Appendix - Modifying Component Server Settings on page 93 for more information about component server settings. 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 15, 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.

At this point, you are ready to install additional Intel® EMA servers, as described in Additional Server Installation on page 49.

2.2.1.13 Modify Server Settings for SAML Authentication

NOTE

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

The following steps are performed on the Server Settings tab of the Intel® EMA user interface. Refer to the Appendix - Modifying Component Server Settings on page 88 for more information about component server settings. These steps must be performed before you can add additional users in SAML 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 SAML Authentication, SAML IDP Entity ID and SAML IDP Metadata URL.
4. The ACS (Assertion Consumer Service) URL is required for SAML authentication configuration. Use this URL format when setting up your Identity Provider: https://<EMA_URL>/saml/acs Replace <EMA_URL> with your actual EMA instance domain.

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. In addition, you can manually recycle your IIS Application pool used on the EMA website.

When these settings are updated to the Intel® EMA Server, you may need to verify log on credentials using SAML SSO credentials.

At this point, you are ready to install additional Intel® EMA servers, as described in Additional Server Installation on page 49. Additionally you may add SAML user as described in Managing SAML Authentication Users on page 72.

2.2.2 Additional Server Installation

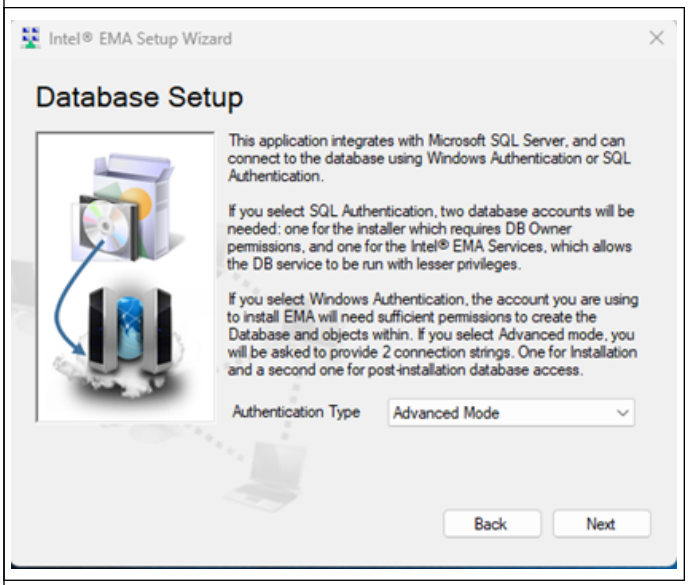
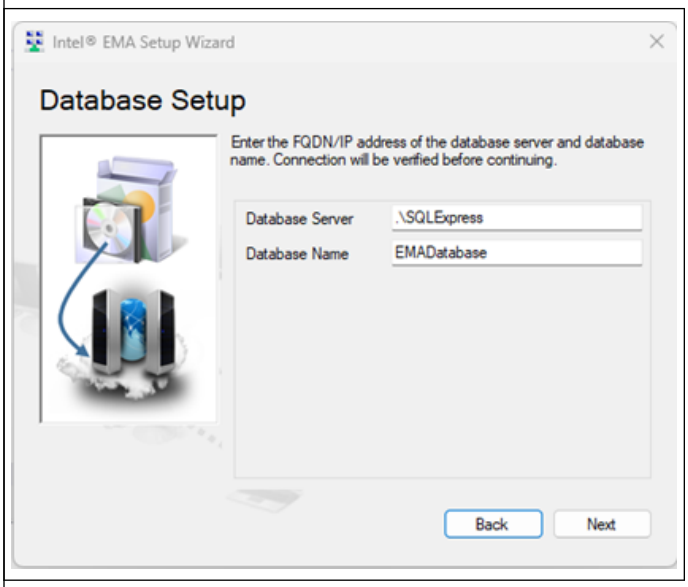
NOTES

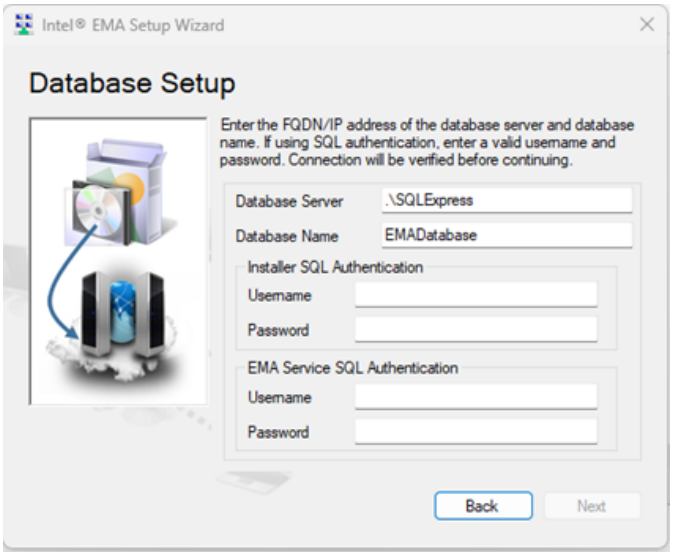
- If you are installing all components on one machine at this time, you do not need to perform the steps in this section.
- You must complete the steps in Initial Server Installation on page 36 before performing the steps in this section (or you can reference any existing Intel® EMA server already in your distributed server architecture).
- By default, the Intel® EMA Platform Manager runs under the System account, and so do the component servers (Ajax server, Swarm server, Recovery Server, Manageability server). In a distributed server installation, these components may need access to a remote SQL Server, in which case you need to change the account these components run under to one that can access the remote SQL Server. Refer Change the Platform Manager Service User Account on page 26 for details on how to configure the account that these services run under.
- The default IIS user account on your Ajax and Web servers will need to be configured with credentials that can access your remote SQL server. Refer IIS – Change IIS User Account on page 23 for details.

.

Run the Intel® EMA installer **EMAServerInstaller.exe** (run as Administrator), choose **Install or Update**, then click **Next** at the Welcome screen. At the Server Host Configuration screen, choose **Additional Server Install for Distributed Server Architecture**.

2.2.2.1 Database Settings

	Select the desired authentication type: Windows Authentication, SQL Authentication, or Advanced Mode. *Note:* 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.
	If you choose Windows Authentication the account you are using for installation will be used to authenticate against the SQL server and create the database. 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. 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.



If you choose 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.

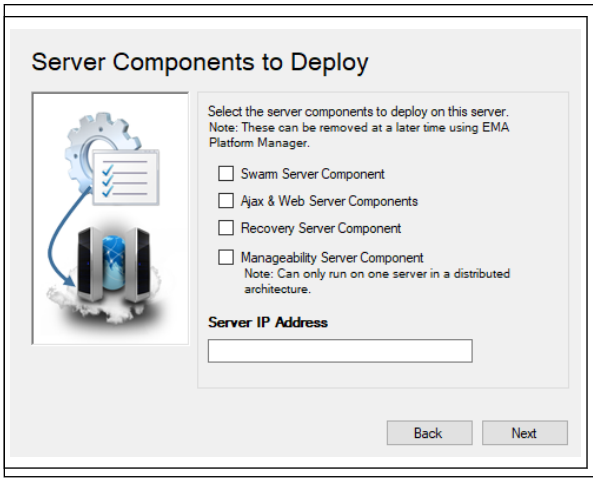
Note: The parameter "MultipleActiveResultSets=True" is required. For more information, refer https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/sql/enabling-multiple-active-result-sets.

The connection string is encrypted and stored in **c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config**.

Important: If installing a distributed server architecture, copy the customized connection strings to a text file to save it for use when installing additional servers.

Note: During an upgrade, the connection information is displayed but cannot be edited as part of the installation flow. Refer Updating the Database Connection String on page 81for information on editing connection strings.

2.2.2.2 Server Components to Deploy- Additional

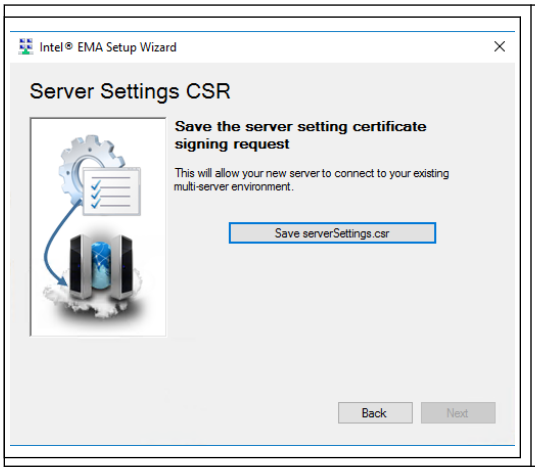


Specify which server components to deploy on this server machine, then verify the **IP Address** of this server machine (field filled in by default).

Note: Only one machine can run the Manageability Server component. If you want to install a Manageability Server component on an additional server, you must remove any other installation of the Manageability Server.

For information about the various server components, refer *Intel® EMA Installed Component*.

2.2.2.3 Save the Server Settings Certificate Signing Request

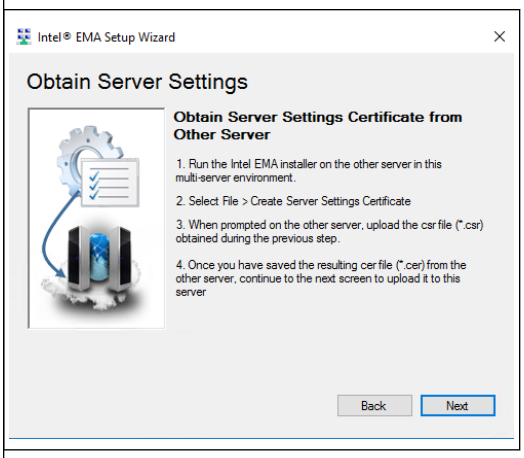


This screen lets you save a Certificate Signing Request (CSR) for the server settings, which is needed to connect your new server to your existing distributed server environment.

1. Click **Save serverSettings.csr**.
2. Select where to save the certificate signing request file.

   Note: Be sure to save the .csr file to a location where it can be accessed from the initial server you installed in Section 1 (such as a shared network drive accessible from both machines or a USB drive).
3. Click **Next**.

2.2.2.4 Obtain Server Setting Certificate

	On the initial server you installed in Initial Server Installation on page 36, perform the steps in Create Server Settings Certificate on Initial Distributed Server Machine on page 53 below. Once you have created the Server Settings Certificate on the initial server, click **Next** to proceed with the Additional Server installation.

2.2.2.4.1 Create Server Settings Certificate on Initial Distributed Server Machine

Perform the following steps on the machine (physical or virtual) where you performed the initial server installation (Section 1). These steps must be completed before proceeding to the next Setup Wizard screen of the additional server installation.

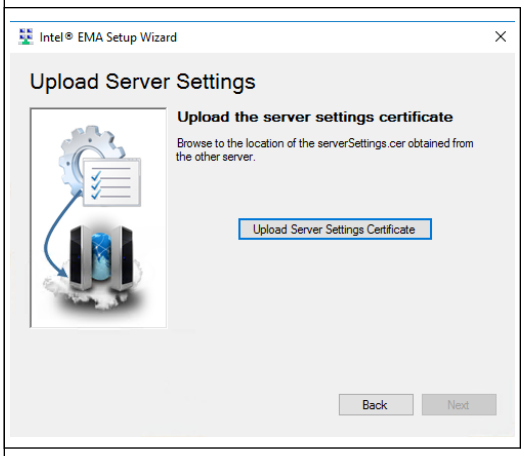
1. Run the Intel® EMA installer, **EMAServerInstaller.exe**. Be sure to **Run as administrator**.
2. From the menu bar at top, click **File > Create Server Settings Certificate**.
3. **Browse** to the location where you saved (or copied) the Certificate Signing Request (.csr) file in Section 1 above.
4. Click **Save Certificate** to save the new certificate (.cer) file.

   NOTE

   Be sure to save the .cer file to a location where it can be accessed from the additional server you are installing (such as a shared network drive accessible from both machines or a USB drive).

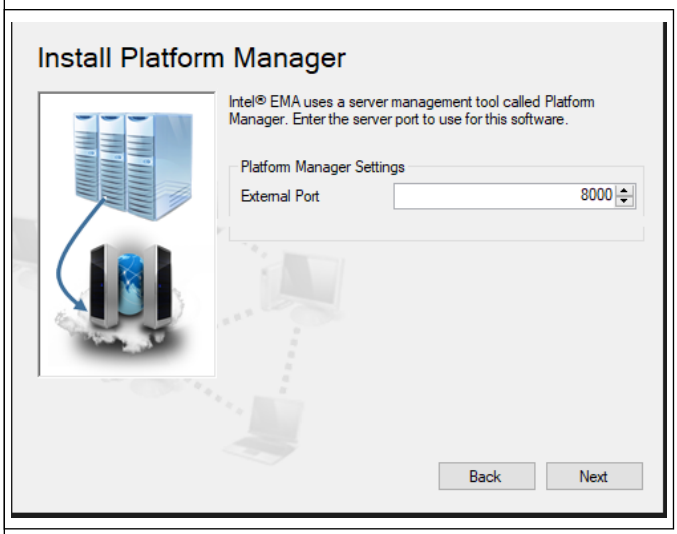
5. Once the "Saved .cer file" message is displayed, click **Exit** to close the dialog, then click **File** > **Exit** on the Intel® EMA Server Installer.

2.2.2.5 Upload Server Setting Certificate



1. Click **Upload Server Settings Certificate**
2. Select the certificate file (.cer) that you created on the initial distributed server machine in the previous step.

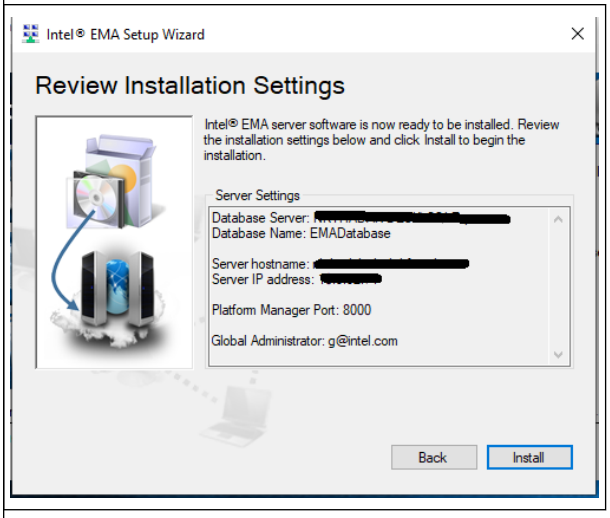
2.2.2.6 Platform Manager Configuration



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.

2.2.2.7 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. Refer section *Using the Global Administrator Interface*

2.2.2.8 Modify IIS Settings If Ajax and Web Server Components Installed

If you selected the **Ajax and Web Server components** on the **Server Components to Deploy** screen during additional server installation above, you need to modify your IIS settings to use the fixed machine keys created on the initial distributed server installation (Initial Server Installation on page 36).

1. In IIS Manager, stop the Default Web Site.
2. Double-click the **Machine Keys** section and set the **Encryption method** to AES and the **Validation method** to one of the SHA-2 family methods (for example, HMACSHA256).
3. Deselect the Generate Keys option, then set the values for the Validation key and the Decryption key to the values used for the initial distributed server (Refer *Create Shared Folder*).
4. Click **Apply** and then restart the Default Web Site.

2.2.2.9 Modify Server Settings

The following steps are performed on the Server Settings tab of the Intel® EMA user interface. Refer Appendix - Modifying Component Server Settings on page 93 for more information about component server settings.

1. Open a browser and navigate to the URL of the Ajax and Web server load balancer that you configured as part of you initial server installation. The Intel® EMA website user interface is displayed.
2. At the login page, enter the user name and password for the Global Administrator. The Overview page is displayed.
3. From the navigation pane at left, select **Settings** to open the Server Settings page.

4. On the Swarm Server tab, click **Add Entry**.
5. For **Server ID**, you will need to review the Intel® EMA database, specifically the [dbo].[ServerSettings] table. The correct Server ID value on this dialog will be the value of **ValueInt** field in the database table with **Type** = 2 and for the server **Name** corresponding to your new additional server.
6. For **IP Address and Port**, if a Swarm Server was selected for installation on this additional server, enter the IP Address of the Swarm Server. For the port, enter the port number (e.g., 8089) that is shown in the **Admin Port** field at the top of the Swarm Server tab. The format for this field is [IP Address]:[Port] (for example, 123.456.789.10:8089).
7. For **Server IPs**, ensure all IP addresses of all physical or virtual servers in this distributed Intel® EMA server environment are listed.
8. Click **Save Settings**. At this time, do not use the **Save and Restart Server** button.
9. Repeat the above process on each of the Ajax and Manageability component server tabs. Note that only the Swarm server tab has the **Admin Port** field, so use the same value in the **IP Address and Port** field on the other server tabs.
10. Once all tabs have been updated, on each server machine in the distributed server environment, run Platform Manager and restart all server components on each machine using Platform Manager's **Halt** and **Launch** commands. Also recycle the Intel® EMA website's IIS app pool if you installed the Intel® EMA Web and Ajax components on that machine. Alternatively, you can restart each server machine in the distributed server environment.

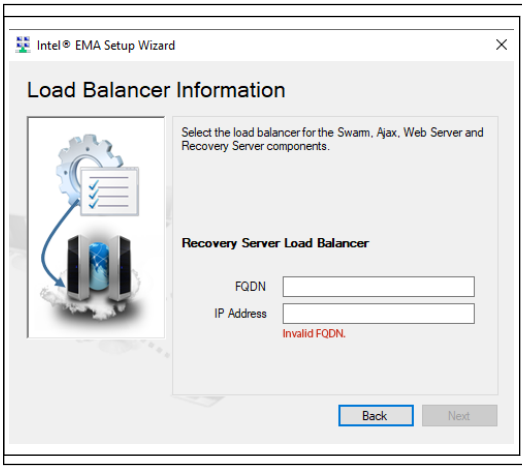
At this point, you are ready to log in as the Global Administrator and click View Getting Started tips under Getting Started on the overview page. Refer Using the Global Administrator Interface on page 70.

2.3 Performing an Update Installation Using the Setup Wizard

NOTES

- If you are updating an existing Single Server Architecture environment, refer "Appendix - Updating a Single Server Architecture Environment" for detailed procedures for this operation.
- If you are updating from an existing version of Intel® EMA, the Intel® EMA website's bindings in IIS will be set to default values during the update installation. You can check the log files after installation to find the pre-update bindings for your reference.
- The Intel® EMA Agent software on managed endpoints is automatically updated upon connecting to the updated Intel® EMA server instance for the first time after server update. For Intel® EMA version 1.5.0 and later, this automatic update is only performed if the Swarm Server setting Agent Auto Update is enabled (default). Refer Appendix - Modifying Component Server Settings on page 93
- For updates from previous Intel® EMA versions, the installer detects the connection string automatically.

2.3.1 Load Balancer Information - Recovery Server

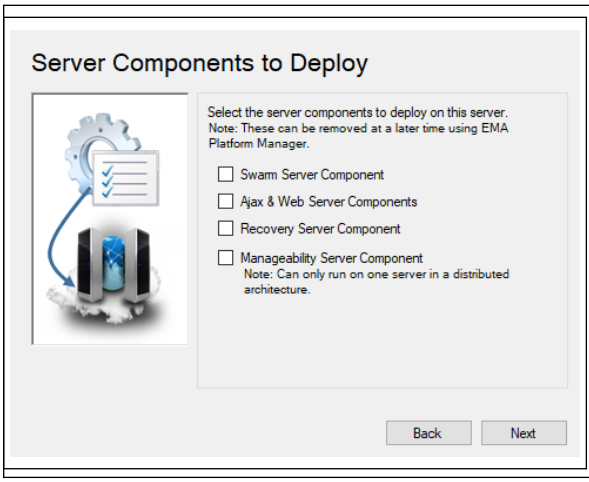


Note: This screen is only displayed during updates from Intel® EMA versions less than v1.6.0.

Enter the **FQDN** and/or **IP Address** (or both, depending on Identity mode) of the load balancer for the Recovery Server component.

Note: A full FQDN is required for One Click Recovery. If you plan to use the One Click Recovery feature, you must enter a complete FQDN (server_name.domain), not just the server name. Also, do not only enter the IP Address if you plan to use One Click Recovery.

2.3.2 Server Components to Deploy

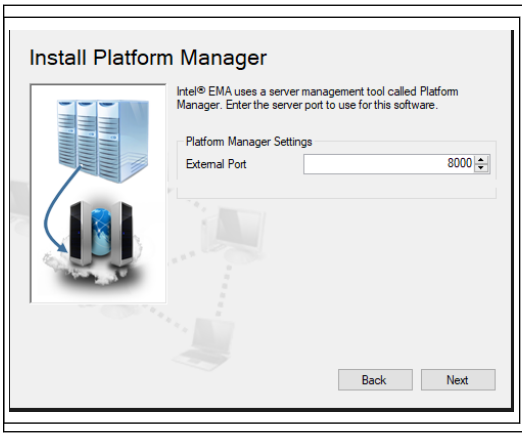


Specify which server components to deploy on this server machine.

Notes:
- Only one machine can run the Manageability Server component.
- Server components already deployed on this machine are shown grayed out and cannot be edited.
- If you select a new component to deploy on this machine, the Server IP Address field is displayed so you can enter this machine's IP Address.

For information about the various server components, refer *Intel® EMA Installed Component*.

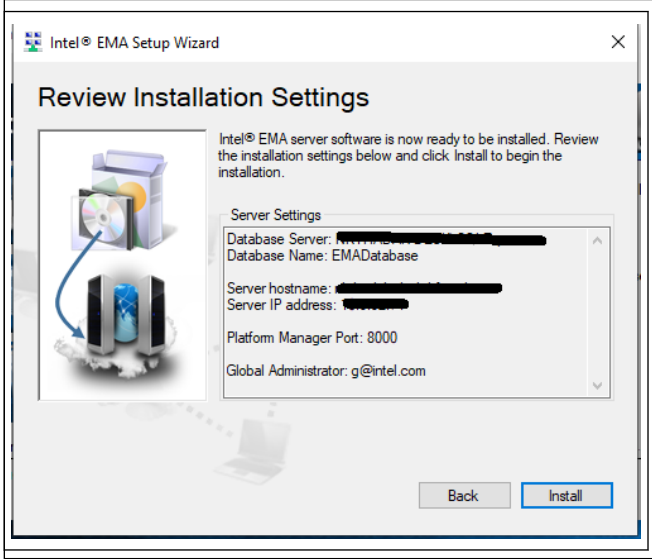
2.3.3 Platform Manager Configuration



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.

2.3.4 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.

2.4 Installing or Updating Using the Command Line

This section describes how to install or update from the command line.

NOTE

The installer requires a relative path to the installer executable EMAServerInstaller.exe. You cannot use an absolute path when issuing the installer command. Change directory to the directory where EMAServerInstaller.exe is located and issue the command from that folder.

There are two modes for command line installation: Basic Mode and Advanced Mode. Use Basic Mode to provide all database connection values directly in the command line. Use Advanced Mode to provide a customized database connection string.

NOTE

Both Basic and Advanced modes create a connection string which is used by the Intel® EMA component servers. Advanced Mode allows you to create a customized connection string.

The connection string is encrypted and stored in c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config.

NOTE

For updates from previous Intel® EMA versions, the installer detects the connection string automatically.

NOTE

During single server standard installation, the Intel® EMA installer creates a folder for use with the USB Redirection (USBR) and One Click Recovery (OCR) features, which allow you to boot a managed endpoint to an image file (.iso or .img) that is stored in this folder. This folder is created with the following permissions: SYSTEM, Administrators, and IIS AppPool\DefaultAppPool. If you alter these permissions, the next time you perform an update installation to Intel® EMA a warning message will be logged informing you that permissions for the folder do not meet requirements.

Open a command prompt in Administrator mode in the folder where you unpacked the installation package.

2.4.1 Initial Installation

Use the command examples in this section to install a distributed server architecture instance of the Intel® EMA server For updates to an existing version, refer section Performing an Update Installation Using the Command Line.

To install the initial server of a distributed server architecture, use the syntax below , substituting correct values for the placeholder values <in brackets> in the example .

```
EMAServerInstaller FULLINSTALL --isdistributedserverinit --
swarmlbhost=<swarmHostLBFQDN> --swarmlbip=<w.x.y.z> --ajaxlbhost=<ajaxHostLBFQDN>
--ajaxlbip=<w.x.y.z> --recoverylbhost=<recoveryHostLBFQDN> --
recoverylbip=<w.x.y.z>--emaip=<current machine IP address> [--ipfirst|--
hostfirst] --dbserver=<dbServer> --db=<dbName> --guser=<UserName> --
gpass=<UserPassword> --deployajaxandweb --deploymanageability --deployswarm --
deployrecovery --createDefaultUsbrFolder --accepteula -c -v
```

NOTE

If you are installing only one server machine at this time, you must use the --createDefaultUsbrFolder flag to ensure the required folder for the USBR feature is created. For more information on this feature, refer Intel® EMA Administration and Usage Guide.

The grouping of descriptions below corresponds to the flow of screens in the installation wizard.

General

FULLINSTALL	indicates that action to perform is installation
-c	to run in console mode, required
-v	for verbose output, optional but recommended
--accepteula	to accept the license agreement, required. The EULA can be viewed in the extracted install package zip in the "Licenses" folder
--help	can be used to view the full help text for the installer

Server Host Configuration

--isdistributedserverinit	Use this flag for initial install for distributed server

Database Settings

NOTE

Two database accounts are required: one of the installer which requires DB Owner permissions, and one for the Intel® EMA services, which allows the database service to be run with lesser privileges.

For the database connection, use the following:

Windows Authentication: `--db=<DBName>` and `--dbserver=<DBServerName>`

SQL Authentication: `--db=<DBName> and --dbserver=<DBServerName> --dbuserinstaller=<UserId>, --dbpassinstaller=<Password>, --dbuserservice=<UserId> and --dbpassservice=<Password>`

The `--dbadvanced` parameters are used to provide a customized database connection string for the installer or the service; the connection strings are encrypted and stored in c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config.

```
--dbadvancedinstaller= "<connection_string>" OR --dbadvancedservice= "<connection_string>"
```

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.

NOTE

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.

Load Balancer Information

For identity mode:

No flag	use FQDN only, provide FQDN only
--hostfirst	use FQDN first, provide FQDN and IP address
--ipfirst	use IP address, provide IP address only

If using FQDN use the following flags:

```
--swarmlbhost=<swarmHostLBFQDN>

--ajaxlbhost=<ajaxHostLBFQDN>

--recoverylbhost=<recoveryHostLBFQDN>
```

If using IP use the following flags:

```
--swarmlbip=<w.x.y.z>
```

```
--ajaxlbip=<w.x.y.z>
```

```
--recoverylbhost=<w.x.y.z>
```

Server Components to Deploy

Use the flags below to select which components to deploy:

```
--deployajaxandweb --deploymanageability --deployswarm --
deployrecovery
```

Also, you must use this flag to set the information for this server IP address:

```
--emaip=<w.x.y.z>
```

User Authentication and Global Admin Account Setup

--guser=<Username> --gpass=<userpassword>	Username/password authentication
--domainauth	Windows domain authentication
--AzureAdauth --guser=<Username> --gpass=<userpassword>	Azure AD authentication
--SamlAuth --guser=<Username> --gpass=<userpassword>	SAML Authentication

Finishing up

--createDefaultUsbrFolder	If you are installing only one server machine at this time, you must use this flag to ensure the required folder for the USBR feature is created.

2.4.2 Add an Additional Server

Overall syntax:

```
EMAServerInstaller FULLINSTALL --isdistributedserveradd --emaip=<current machine
IP address> --dbserver=<dbServer> --db=<dbName> --
certimeoutseconds=<timeOutSeconds> --csrfile=<csrFilePath> --
cerfile=<cerFilePath> --deployajaxandweb --deploymanageability --deployswarm --
deployrecovery --accepteula -c -v
```

General

FULLINSTALL	indicates that action to perform is installation
-c	to run in console mode, required
-v	for verbose output, optional but recommended
--accepteula	to accept the license agreement, required. The EULA can be viewed in the extracted install package zip in the "Licenses" folder
--help	can be used to view the full help text for the installer

Server Host Configuration

--isdistributedserveradd	Use this flag for additional distributed server install.

Database Settings

NOTE

Two database accounts are required: one of the installer which requires DB Owner permissions, and one for the Intel® EMA services, which allows the database service to be run with lesser privileges.

For the database connection, use the following:

Windows Authentication: `--db=<DBName>` and `--dbserver=<DBServerName>`

SQL Authentication: `--db=<DBName> and --dbserver=<DBServerName> --dbuserinstaller=<UserId>, --dbpassinstaller=<Password>, --dbuserservice=<UserId> and --dbpassservice=<Password>`

The `--dbadvanced` parameters are used to provide a customized database connection string for the installer or the service; the connection strings are encrypted and stored in c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config.

```
--dbadvancedinstaller= "<connection_string>" OR --dbadvancedservice= "<connection_string>"
```

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.

NOTE

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.

Server Components to Deploy

Use the flags below to select which components to deploy:

```
--deployajaxandweb --deploymanageability --deployswarm --deployrecovery
```

Also, you must use this flag to set the information for this server IP address:

```
--emaip=<w.x.y.z>
```

Save the Server Settings Certificate Signing Request

--csrfile=<csrFilePath>	Path to save the CSR file. If not provided default value of ".\serversettings.csr" will be used.
--certimeoutseconds=<timeOutSeconds>	Timeout value to pause waiting for CER file.

Upload Server Settings Certificate

--csrfile=<cerFilePath>	Path for the CER file. If not provided default value of ".\serversettings.cer" will be used.

To install an additional server in a distributed server architecture, perform the following steps, substituting correct values for the placeholder values <in brackets> in the examples.

1. Begin the installation on the additional server machine by entering the above command using the flags as described. The installation will pause in order to consume the files created in the remaining steps. The installer command will pause for the length of time specified in the `--certimeoutseconds` option. Note that if --csrfile option is not provided, the default of `.\serversettings.csr` will be used (same for the cerfile, but with a .cer extension).
2. When the installer pauses, copy the generated certificate request (.csr) file to the initial server machine.
3. On the initial server machine, run the installer with the createsettingscert option, as shown below: `EMAServerInstaller CREATESETTINGSCERT --csrfile=<csrFilePath> --cerfile=<cerFilePath> -c -v -a`

   NOTE

   Alternatively, you can run the Intel® EMA installer setup wizard on the initial server and click **File > Create Server Settings Cert**, as described in Section Obtain Server Setting Certificate.

4. On the initial server, copy the resulting certificate (.cer) file to the additional server machine. Or you can specify a shared folder accessible by both machines to save the .cer file to in the previous step, as long as you specify the same location in the --cerfile option of the installer command in step 1 above.
5. On the additional server, the installation will automatically continue once it detects the certificate (.cer) file in the location specified in the `--cerfile` option.

2.4.3 Performing an Update Installation Using the Command Line

NOTES

- If you are updating an existing Single Server Architecture environment, refer Appendix - Updating a Single Server Architecture Environment on page 109 for detailed procedures for this operation.
- When upgrading an Intel® EMA instance, the account under which the Platform Manager service runs reverts to Local System. If you are running that service under another local or domain account, it will need to be reconfigured and all Intel® EMA components halted and restarted after the upgrade is complete.
- The Intel® EMA Agent software on managed endpoints is automatically updated upon connecting to the updated Intel® EMA server instance for the first time after server update. For Intel® EMA version 1.5.0 and later, this automatic update is only performed if the Swarm Server setting Agent Auto Update is enabled (default). Refer Appendix - Modifying Component Server Settings on page 93 for details.
- For updates from previous Intel® EMA versions, the installer detects the connection string automatically.
- Once installed EMA, you can't change to SAML authentication. If you need to use a different authentication method, you will need to perform a fresh installation, there is no EMA upgrade support.
- For updates from previous Intel® EMA versions, the installer detects the connection string automatically.

Use the command example below to update the Intel® EMA server machine.

```
EMAServerInstaller FULLINSTALL --updateinstalltype=<single/
distributed> --accepteula -c -v
```

NOTES

- For updates from previous Intel® EMA versions, only the updateinstalltype, accepteula, console (c), and verbose (v) parameters are accepted. Do not enter any other parameters for updates. Doing so will cause the installation to abort and an error message to be displayed.
- For updateinstalltype, you must correctly specify which type of installation (single server architecture or distributed server architecture) you are currently updating. **Specifying the wrong type will result in an inoperable Intel® EMA instance which must be fully uninstalled and reinstalled.**

2.4.4 Converting to Azure AD Using the Command Line

IMPORTANT

It is HIGHLY recommended that you perform a backup of the Intel® EMA database BEFORE using this command. The switch cannot be undone, but you can manually restore your database from the backup if you decide you want to reverse this action.

Use the command example below to convert your existing Intel® EMA installation from Windows Authentication to Azure AD Authentication. A root Global Administrator account will be created during this process.

For the username you can specify a username of an existing Global Admin account, or you can choose to create a new username for the root Global Admin account. You must provide a password to use with this root Global Admin account, and all future logins to Intel® EMA with this account will use username/password to login.

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.

After using this command, restart the Web Server (or recycle the application pool) for each Intel® EMA website on each machine on which the Web Server is installed (note that it is not sufficient to simply restart the web site). Use IIS Manager to do this.

After using this command and restarting the Web Servers in IIS, go to the Intel® EMA login page and refresh the page at least twice. At this point the Azure AD SSO login option should be displayed.

```
EMAServerInstaller SWITCHTOAZUREAD --guser=<UserName> --gpass=<UserPassword> -c -v
```

`--guser=<UserName>` specifies the username to use for root Global Admin account. This can be a new username or the username of an existing Global Admin account.

`--gpass=<UserPassword>` specifies the password to use for the root Global Admin account.

2.5 Uninstalling

Do not abort or exit the installer before the uninstallation is complete.

NOTE

- Before uninstalling, ensure the account used in the Intel® EMA SQL connection string has at least db_creator rights, which allow it to create, modify, and delete any database. This account must also have the database level roles db_owner, db_datawriter, and db_datareader.

2.5.1 Uninstalling Using the Installer GUI

1. On the Installer main menu, click the **Uninstall the Intel® EMA Server** option at bottom.
2. On the dialog, decide whether you want to delete the settings certificate.
3. Decide whether you want to delete the database.

WARNING

If this is a distributed server architecture installation, this option will make the entire Intel® EMA instance unusable. Use this option only if this is the last remaining server.

NOTE

If the database is managed and/or cloud-based, Intel® EMA cannot delete the database so do not specify this option.

NOTE

In a single server installation, this option will also remove the default shared USBR image file storage folder. If you specify a custom USBR image storage folder in Server Settings, that folder will not be deleted.

If the database is managed and/or cloud-based, Intel® EMA cannot delete the database so do not specify this option.

4. Click **OK**, then click **OK** to the warning message.
5. After the uninstall is complete, check the log by clicking **File > Advanced Mode** to confirm successful completion.

2.5.2 Uninstalling Using the Command Line

NOTE

The installer requires a relative path to the installer executable EMAServerInstaller.exe. You cannot use an absolute path when issuing the installer command. Change directory to the directory where EMAServerInstaller.exe is located and issue the command from that folder.

1. Open a command prompt window with administrative privileges.
2. Change directory to where the Intel® EMA Installer Package was extracted.
3. To uninstall without removing the database and settings certificate, type the **UNINSTALL** command below and press **Enter**.

   ```
   EMAServerInstaller UNINSTALL -c --verbose
   ```

4. To uninstall and remove the settings certificate, add the `--deletesettingscert` option.

   ```
   EMAServerInstaller UNINSTALL --deletesettingscert -c --verbose
   ```

5. To uninstall and remove the database, add the --deletedb option, shown below (to remove both the settings certificate and the database, use both options).

   ```
   EMAServerInstaller UNINSTALL --deletedb -c --verbose
   ```

WARNING

If this is a distributed server architecture installation, this option will make the entire Intel® EMA instance unusable. Use this option only if this is the last remaining server.

NOTE

If the database is managed and/or cloud-based, Intel® EMA cannot delete the database so do not specify this option.

NOTE

In a single server installation, this option will also remove the default shared USBR image file storage folder. If you specify a custom USBR image storage folder in Server Settings, that folder will not be deleted.

If the database is managed and/or cloud-based, Intel® EMA cannot delete the database so do not specify this option.

2.6 Intel® EMA Installer Advanced Mode Menu Bar

By default, the Intel® EMA installer **EMAServerInstaller.exe** menu bar has two choices: **File** and **Help**. Selecting **File > Advanced Mode** displays an expanded menu bar with the following menu choices.

File	**Advanced Mode** Sets Advanced Mode on, displays expanded menu bar, and displays a log file of installer actions that have occurred (for using during or after installation).
Database	**Update Database** Launches the Update Database Settings dialog. Use this to update your database connection string post-installation.
Settings	**Sync Web Server Settings** Restarts the Intel® EMA Web Server to apply/sync changes to web server settings. **Fix Settings Issues** Checks the server settings in the Intel® EMA database. If any server settings are missing, it will add the missing ones with the default values. This process is also automatically performed during an Intel® EMA version update install. **Switch from LDAPS to LDAP** Sets the LDAP ports Intel® EMA uses to the standard non-secure ports. 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. See the following link for more information: https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts. Switch from Windows AD to Azure AD

continued...

	Important: It is HIGHLY recommended that you perform a backup of the Intel® EMA database BEFORE using this command. The switch cannot be undone, but you can manually restore your database from the backup if you decide you want to reverse this action. Updates internal Intel® EMA settings to switch this instance of Intel® EMA from Windows AD authentication to Azure AD authentication. You will be prompted to create a new root Global Administrator account. For the username you can specify a username of an existing Global Admin account, or you can choose to create a new username for the root Global Admin account. You must provide a password to use with this root Global Admin account, and all future logins to Intel® EMA with this account will use username/password to login. After using this switching tool, restart the Web Server (or recycle the application pool) for each Intel® EMA website on each machine on which the Web Server is installed (note that it is not sufficient to simply restart the web site). Use IIS Manager to do this. After using the switching tool and restarting the Web Servers in IIS, go to the Intel® EMA login page and refresh the page at least twice. At this point the Azure AD SSO login option should be displayed. *Notes:* • You MUST have Intel® EMA v1.9.0 or later installed in order to use this option. In a distributed environment, all Intel® EMA server machines must be updated to v1.9.0 or later. • The current Authentication Type must be Windows AD, not local (normal) accounts. • Any existing Windows AD users that are not in your Azure AD tenant will no longer be able to login to Intel® EMA after the switch. • You will not be able to add users and other Intel® EMA actions until you perform the steps in section 1.4 in Azure AD.

continued...

Actions	**Setup Firewall Rules** Runs the portion of the installer that handles firewall rule configuration. **Clear Firewall Rules** Runs the portion of the uninstaller that resets firewall rules. **IIS Registration** Runs the Microsoft.NET aspnet_regiis.exe **Dump all features to file** Writes the enabled Windows features to a file, and writes disabled Windows features to another file. **Check Common Names** Displays the hostname, FQDN, IP addresses of this machine. **Check Software** Displays IIS version, .NET CLR version, OS version, .NET framework. **Domain Detection** Detects what domain the system running the installer is part of. **Download disallowed password list** Downloads the current disallowed password list. **Upload disallowed password list** Allows user to upload a new disallowed password list. *Note:* File format must be UTF-8 encoded text file, with newline delimiter separating each disallowed password. **Lock/Unlock local global admin account** Enables or disables the local Global Administrator account (global root account), so that it cannot login to the Intel® EMA Web UI or Platform Manager when disabled. The account is not removed, and can be re-enabled in the future. This option is only applicable to installations using Azure AD authentication. **Uninstall the Intel® EMA Server** Uninstalls the Intel® EMA server.
Manager	**Launch Intel® EMA Platform Manager** Launches the Intel® EMA Platform Manager
Help	**Intel Support** Opens the Intel support portal in a web browser.

3.0 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.

NOTE

In order to perform the Tenant setup tasks as described in the section 3 of the Intel® EMA Administration and Usage Guide, you must be logged in as the Tenant Administrator user of that Tenant. See the Intel® EMA Administration and Usage Guide for details.

Logging out

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

3.1 Changing the Global Administrator Password

This operation can only be performed if "normal accounts" or Azure AD authentication mode was selected during installation.

In the top right of the title bar, click the circle showing the first two letters of the Global Administrator user name and select **Change password**.

3.2 Creating and Deleting Tenants

To create a new Tenant, do the following:

1. From the **Overview** page, click **Create a tenant** under **Tenants** at bottom left. Or, from the **Getting started** page (available by clicking **View Getting Started** tips on the first page), select the **Create Tenant**.
2. Enter a **Tenant Name** and Description, then click **Save**.

To delete a Tenant, select the Tenants tab on the Users page, then click the down-arrow at right for the target Tenant and select **Delete Tenant....**

3.3 Managing Users and User Groups

To manage users or user groups, you must first select a target tenant. New users (except for a new global administrator) and user groups are created under this target tenant.

3.3.1 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.

3.3.2 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 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.

3.3.3 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**.

3.3.4 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.

3.3.5 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 71.

4.0 Performing Intel® EMA Server Maintenance

Use the Intel® EMA Platform Manager to monitor each Intel® EMA server and perform various maintenance tasks on the component servers running on the Intel® EMA server machine. You can also use it to deploy a new Intel® EMA component server package. In a distributed server architecture environment, a Platform Manager client on one Intel® EMA server machine can connect to and monitor the server components on the other Intel® EMA server machines.

NOTE

Be sure to change the user account under which the Platform Manager service runs. Refer Disable Insecure Cipher Suites for details.

Intel recommends following security best practices, including installing Platform Manager in the suggested default location. Otherwise, be sure to install and run Program Manager in a system privileged folder on the target system.

4.1 Manually Installing Platform Manager

The Platform Manager tool is installed as part of the Intel® EMA server installation. However, if necessary, you can install it manually by opening the Intel® EMA installation media and running the Platform Manager installation file **PlatformManager.msi** (be sure to run as Administrator).

You can use this method to install a standalone Platform Manager client on a Windows-based machine separate from the one on which the Intel® EMA server is installed, then remotely connect from the standalone Platform Manager client to the existing Platform Manager server on the Intel® EMA server machine.

Additionally, you can use this method to reinstall the Platform Manager server in the event that it gets accidentally uninstalled. This assumes that all other Intel® EMA components are still installed in **C:\Program Files (x86)\Intel\Platform Manager** and that you reinstall Platform Manager to the same location.

4.2 Configuring the Intel® EMA Platform Manager Service

Before using the Platform Manager, review this section and decide if you want to modify any default settings. All of the configurable values are in the file C:\Program Files (x86)\Intel\Platform Manager\Platform Manager Server\settings.txt.

4.2.1 Platform Manager TLS Certificate

The Platform Manager Service provides the TCP TLS connection between the service and the client application. A default certificate for this TLS connection is provided with the Intel® EMA installation, but this default certificate can be updated to a certificate from a reputable certificate authority by updating the “certhash” value in the settings.txt file with the thumbprint of the TLS certificate you want to use.

4.2.2 Mutual TLS Certificate for Client Authentication

The Platform Manager Service can optionally require that Mutual TLS be used in the connection between the service and client applications. To enable this, update the "allowedclientcert" value in the settings.txt file with the client certificate thumbprint. Multiple client certificates are supported by adding multiple "allowedclientcert" lines.

When you enable this feature, only clients providing a certificate which corresponds to one defined in the "allowedclientcert" list will be allowed to connect.

4.2.3 Kerberos with Active Directory in a Distributed Server Installation

If you are using Kerberos and Active Directory in a distributed server installation, then to connect the Platform Manager service without having to make multiple HOST file entries on the servers and restart the Platform Manager service on each, ensure the load balancer has been added as a Service Principal Name (SPN) for the computer account in Active Directory. For more information on SPNs refer the following link: https://techcommunity.microsoft.com/t5/iis-support-blog/service-principal-name-spn-checklist-for-kerberos-authentication/ba-p/347639

4.3 Using the Intel® EMA Platform Manager Client Application

Once you have configured the Platform Manager service, you are ready to start using the Platform Manager client application.

4.3.1 Starting Intel® EMA Platform Manager

NOTE

If you are using Intel® EMA in a Microsoft Azure AD authentication environment, before performing the steps in either section below, ensure that the Microsoft Edge WebView2 Runtime component is installed. Some versions of Windows have this component preinstalled. If WebView2 is not installed, click the link below and follow the instructions to download and install it before performing the steps to start Platform Manager.

https://developer.microsoft.com/en-us/microsoft-edge/webview2/

4.3.1.1 From the Intel® EMA Installer

When you launch Platform Manager from the Intel® EMA installer, the installer automatically detects the Intel® EMA server connection information as well as your login authentication method.

1. Run the Intel® EMA installer **EMAServerInstaller.exe** (run as Administrator) and click the Launch Intel **EMA Platform Manager** button.
2. If you are using Windows Authentication, the connection credentials are automatically detected and used, and the Platform Manager window is displayed with the application servers shown in the left-hand pane.

3. If you are using Azure AD authentication or Intel® EMA credentials, the **Connection Credentials** dialog is displayed, with the detected authentication method selected. Click **Next** to complete the Azure AD sign on process or enter Intel® EMA user credentials for the Global Administrator user.
4. If you are using SAML authentication or Intel® EMA credentials, the Connection Credentials dialog is displayed, with the detected authentication method selected. Click Next to complete the SAML login process or enter Intel® EMA user credentials for the Global Administrator user.
5. The Intel® EMA Platform Manager window is displayed, with the application servers shown in the left-hand pane.
6. To connect to additional servers (in a distributed installation), click **Connect to Server....**

4.3.1.2 From Windows

Follow the steps below to start Platform Manager from Windows (i.e., the Start Menu or Windows Explorer, etc.).

1. Start the Intel® EMA Platform Manager application like any other Windows desktop application.
2. If this is the first time launching Platform Manager, click **Connect to Server...** at the bottom of the screen. Otherwise, if you have previously saved connection and authentication information in a Platform Manager solution file, you can select **File > Load Solution** from the menu bar and choose which file to load (refer section below). If you loaded a file, enter any required credential information and skip to step 12.
3. In the **Connect to Platform Manager Server** dialog, enter the identifier (hostname/FQDN/IP Address) and port for the Intel® EMA Platform Manager server. If you are on the same machine as the Intel® EMA component servers, use the localhost:port value.
4. Enter the **Intel® EMA Web Server Identifier**. This is the hostname/FQDN/IP Address you use to open the Intel® EMA website.
5. If you configured the service for Mutual TLS, select a **Client Authentication Certificate**.
6. Click **OK**.
7. If prompted, verify and **Accept** the Server Certificate.
8. In the **Connection Credentials** dialog, select the connection method: Intel® EMA Credentials, Azure AD Authentication, or Windows Authentication.
9. For Intel® EMA Credentials, enter the username and password for the Global Administrator user.
10. If you are using Windows Authentication, you may get an error connecting to the Intel® EMA server. Check to ensure you entered the correct identifier for the Platform Manager server above, and that the Intel® EMA server is up and running.

NOTE

- If you are using Windows Authentication, ensure the system running Platform Manager is joined to the domain, and that the Global Administrator account you are using is logged into the domain. Otherwise you will be prompted for credentials.

11. For Azure AD Authentication or SAML Authentication, you will be prompted for your Azure AD/SAML Single Sign On (SSO) credentials.
12. The Intel® EMA Platform Manager window is displayed, with the application servers shown in the left-hand pane. If the screen prompts you to **Connect**, check to ensure you entered a user with Global Administrator rights in the Connection Credentials dialog. To connect to additional servers (in a distributed installation), click **Connect to Server...** again.
13. When you exit Platform Manager, if you changed server connection information, you will be prompted to "save solution". You can save the connection and authentication method information to a file and then load that information from the file by using the **File > Load Solution** menu choice the next time you start Platform Manager. Refer section below.

4.3.2 The File Menu

Load Solution	Loads the server connection information from a previously saved file. Launches the Connect to Platform Manager Server dialog with all information pre-filled except for passwords. For Windows and Azure AD/SAML authentication, you will be prompted for sign on credentials.
Save Solution (as...)	Saves the current server connection information to a specified file. This file can then be loaded the next to you start Platform Manager. Passwords are not saved in the connection information (i.e., solution) file.
Add Server	Launches the Connect to Platform Manager Server dialog for you to enter connection information and credentials.
Add Group	Launches the Create Group dialog, where you can group multiple server connections.
Log	Displays the Platform Manager log file.
Exit	Exits the Platform Manager client application.

4.3.3 Monitoring Component Server Events

1. Select a component server from the list in the left-hand pane (for example, the EMAAjaxServer).
2. Select the **Events** tab to see the events for that server. Events are also logged in **C:\Program Files (x86)\Intel\Platform Manager\EMALogs\EMALog-[server type].txt** on the selected server machine. Note that the log file contains more detail than what is displayed on the Events tab.
3. If desired, click **Trace** at the bottom of the panel to enable detailed debugging tracing (this will result in a lot more messages being logged). The trace log is also logged in **C:\Program Files (x86)\Intel\Platform Manager\EMALogs \TraceLog-[server type].txt**.

NOTE

The trace file will not be present if tracing is not enabled for the selected component server.

4.3.4 Monitoring Component Server Internal Tracking Information

1. Select a component server from the list at left.

2. Select the Component tab to display useful information for the selected component server. Different component servers have different tracked values, as described below.

Intel® EMA AJAX server:

- **AjaxSessions:** Number of active AJAX request sessions issued by Intel® EMA JavaScript library, which are process by the AJAX server.HttpSessions: Number of HTTP sessions (used for web redirection features) issued by Intel® EMA JavaScript library, which are process by the AJAX server.
- **SwarmSessions**: Number of active TCP connections to the Swarm server from the AJAX server.
- **WebSocketSessions:** Number of active Web Socket sessions issued by Intel® EMA JavaScript library, which are process by the AJAX server.

Intel® EMA Manageability server:

- Each row is a slot to be used for Intel AMT provisioning. A pending Intel AMT provisioning request is put into an available slot. The Manageability server starts the provisioning for all the slots individually. If there is no slot available, the request awaits for an available slot to open. The row displays the information text of Intel AMT provisioning.

Intel® EMA Swarm server:

- **ConAgents:** Number of active Intel® EMA Agent's TCP connections to the Swarm server.
- **ConConsoles:** Number of active TCP connections from other Intel® EMA servers.
- **ConIntelAmt:** Number of active Intel AMT CIRA connections to the Swarm server.
- **DbFails:** DB queries' failure count made by this Swarm server.
- **DbQueries:** DB query count made by this Swarm server.

4.3.5 Performing Basic Controls on Component Servers

To halt/stop or resume an component server, right-click the server in the left-hand pane and select the desired option.

To see the available control commands for a particular component server, select a server and go to its Console tab, then type "help" and click **Send**. The commands are listed below.

All servers:

- **testmessage**: This sends out test blast messages via TCP connections between Intel® EMA components. You should see the Received test blast from: [source server] message in the Events tab of the AJAX server, Manageability server, and the Swarm server.
- **echo**: Print back what you typed.
- **time**: Print the current server machine time.
- **utctime**: Print the current server machine time in UTC
- **version**: Print the component version.
- **shutdown**: This will let you shutdown/halt this server; however, it will be re-launched soon after.

- **collect**: Trigger .NET garbage collection.
- **whoami**: Print the current account this server runtime is running under.
- **logpath**: Print the log folder path.
- **trace**: Lets you start/stop tracing info being logged in a trace file. The trace file is in the path specified by logpath.
- **restart**: Restarts the server.

Intel® EMA AJAX server:

- **stats**: Print the "tracked values", same as what Application tab shows.
- **testdb**: Test connection to Intel® EMA server DB.
- **ajaxcert**: Print information about the inter-service TLS ajax certificate.
- **swarmsessions**: Print the current swarm sessions.
- **alertsessions**: Print the current alert sessions.
- **dbcount**: Control DB trace counting.
  - **Start**: This starts to collect the database SQL commands info, run by the Swarm server. It includes the collection start time, the collection duration, and the total number of DB connections made by Swarm server. For each SQL command item, it includes the execution count, the error count, the total running time, and the SQL command. **Note** that our SQL commands are designed to use parameterized inputs. Therefore, we only log the parameter name here, not the value.
  - **Save and Restart**: Save the collected data to the EMALogs folder in the Intel® EMA server installation folder.
  - Cancel: Cancel the data collection and do not save anything to file.
- **mcount**: Print the count of different types of test blast messages sent via TCP connections between Intel® EMA components.

Intel® EMA Manageability server:

- **testdb**: Test connection to Intel® EMA server DB.
- **exec**: This triggers the Manageability server to check Intel® EMA server DB to find any Intel AMT provisioning work to be done immediately. Otherwise, Manageability server checks that periodically.
- **restart**: Restart the Manageability server.
- **dbcleanup**: Performs on-demand database maintenance routine. Refer Periodic Database Maintenance on page 83
- **slots**: Print activation tasks' slots. Manageability server currently is performing internal throttling. It can do at most concurrent 20 provisioning tasks (slots). For the remaining provisioning tasks, they will wait in the Intel® EMA sever DB to be picked up later.
- **manageabilitycert**: Displays information about the inter-service TLS manageability certificate.
- **fileuploadcleanup**: Performs on-demand clean up to remove expired USBR temporary files.
- **cert8021xrenewal**: Performs on-demand certificate renewal for expiring 802.1x certificates.

Intel® EMA Swarm server:

- **stats**: Print
  - The incoming traffic from Intel® EMA Agent in bytes, the outgoing traffic to Intel® EMA Agent in bytes.
  - .Net Garbage Collector: GetTotalMemory's value. Intel® EMA DB queries count, connections count, DB queries failure count made by this Swarm server.
  - Connected Intel® EMA agent counts.
  - The number of received blast messages, the number of sent blast messages.
  - Intel® EMA server DB schema version.
- **testdb**: Test connection to Intel® EMA server DB.
- **swarmcert**: Display information about the inter-service TLS swarm server certificate.
- **servercert**: Display information about the Intel® EMA swarm server certificate.
- **resetagentstore**: Sync the in-memory agent installers information based on the available Intel® EMA agent installers in Intel® EMA DB. Then it checks the agent download and agent upload for each connected Intel® EMA agents.
- **forcedisconnect**: This will disconnect this target endpoint for now. The endpoint can still connect back.
- **dbcount**: Control DB trace counting.
- **consoles**: This lists the current connected Intel® EMA application servers. For example, when you do a "remote terminal" session, there will be 1 console session between AJAX Server and Swarm server.
- **dbschema**: Print the Intel® EMA server DB schema version.
- **allownode**: Add an endpoint to pass list. When Swarm server gets an Intel® EMA agent connection request, if there exists a non-empty endpoint banned list, it will check it. If this incoming agent/endpoint is banned, it will reject the connection.

  NOTE

  The current Intel® EMA release does not implement this feature.

- **swarmid**: Print the this Swarm server's id and the lead Swarm server's id. This is useful when you have multiple Swarm servers under load balancer. The leader is usually the Swarm server just started recently and with highest ID.
- **agentpingtime**: Print the current ping time for maintaining Intel® EMA agent TCP connection. If you provide a numerical argument, it will set the ping time to this value in seconds.
- **agentrequireping**: Print if we need all the Intel® EMA agents to respond with a pong to a ping sent by the Swarm server. 1 is true, and 0 is false. If this setting is true, then the Swarm server will drop the agent TCP connection if a pong is not received. If you provide an argument (1 or 0), you can set the value.
- **ignoredupagents:** By default, this is disabled. When the Intel® EMA Swarm server receives an incoming Intel® EMA agent connection, if this connection has an endpoint ID that is the same as an existing connection, then we will disconnect and remove the existing connection and accept the new one. However, if this is

enabled, we will do nothing and just ignore the new incoming connection. This prints 1 or 0. 1 is true/enabled, and 0 is false/disabled. If you provide an argument (1 or 0), you can set the value.

- **swarmpeers**: Print the other peer Swarm servers' IDs and IP addresses.

4.4 Deploying New Packages

A package is a zip file containing a component server or website. An Intel® EMA release contains several packages. Packages are located in the StoredPackages folder in your Intel® EMA release.

NOTE

If you have an older version of Intel® EMA, you can use Platform Manager to upload and deploy newer versions without touching your Intel® EMA database. However, if the new release includes Intel® EMA database changes, then you must still use the Intel® EMA installer to perform an update.

To update a particular component server:

1. In the left-hand pane, open **Intel® EMA Servers** and select a machine from the list (for example, localhost).
2. Select the **Storage** tab.
3. Click **Upload** and select the .zip package (for example, EMASiteCoreReact.zip) you want to deploy to that machine. The old version is replaced with the new version in the Component Packages list.
4. Click **Deploy** to deploy the new package on the selected machine.

4.5 Updating the Database Connection String

NOTE

Two database accounts are required: one of the installer which requires DB Owner permissions, and one for the Intel® EMA services, which allows the database service to be run with lesser privileges.

To update the database connection string after installation, do the following:

1. Run the Intel® EMA Installer Wizard (in the installation folder, right-click on **EMAServerInstaller.exe** and select **Run as administrator**).
2. From the **File** menu, select **Advanced Mode**. Additional menus are displayed, including the Database menu.
3. From the **Database** menu, select **Update Database**. The **Update Database Settings** dialog is displayed.
4. To update the server or database name, or the SQL authentication user and password, simply enter new values for these fields and click Update. To enter a new customized database connection string, continue to the next step.
5. Click the checkbox for **Advanced Mode**.

6. Enter a new Connection String for either connection string field, or both. For more information about connection strings, refer https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax.

NOTE

some examples on this page may not be supported by Intel® EMA.

NOTE

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.

7. Click **Update** to update the connection string and close the Update Database Settings dialog.

NOTE

You must restart all Intel® EMA component servers (i.e., Swarm Server, .Manageability Server, etc.) in order for the new connection string to take effect.

A copy of the previous connection string file **c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config** is created.

In a distributed server architecture environment, the connection string must be updated on all Intel® EMA server systems.

4.6 Revoking a Server's Certificate

In a distributed server architecture environment, there may be situations where you want to revoke an Intel® EMA server's certificate. For example, if you suspect a server has been compromised, or if you plan to decommission a server.

The following certificates (installed in the Personal certificate store on the local Windows machine) can be revoked:

- **Inter-component TLS certificates:** These certificates are used for communication between Intel® EMA components (Ajax server, Swarm server, etc.), as well as between Intel® EMA server machines in a distributed server installation. They can be identified by the value "EmaMtlsXXX" in the **IssuedTo** field, and the value "MeshRoot-XXXX" in the **IssuedBy** field.
- **Intel® EMA settings certificates:** These certificates are used to read the encrypted Intel® EMA server settings in the Intel® EMA database. They can be identified by the value "MeshSettingsCertificates-XXX" in the **IssuedTo** field, and the value "MeshRoot-XXXX" in the **IssuedBy** field.

IMPORTANT

If you revoke the Intel® EMA settings certificate on a single server installation (or on the last server of a distributed server architecture), you will render the Intel® EMA server inoperable. This cannot be recovered and requires fully reinstalling the Intel® EMA server using the installation wizard or the command line installation.

The Intel® EMA API provides an API called **CRL**, which stands for Certificate Revocation List. This API essentially adds a certificate's serial number to a "blocklist" file of certificates known as a Certificate Revocation List.

To use this API to revoke a server's certificate, consult the Intel® EMA API Guide or review the API documentation online in Swagger. Then use a tool like "cURL" to issue the CRL API commands at a command prompt window.

NOTE

The CRL API includes the option to restart the Intel® EMA server components automatically (default) or manually. The automatic option restarts all Intel® EMA component servers (Ajax server, Swarm server, etc.), including the IIS app pool that hosts the Intel® EMA website.

NOTE

Any other websites in that app pool will be restarted as well. The automatic option restarts all components on all servers in a distributed server architecture.

4.7 Periodic Database Maintenance

The Intel® EMA database grows over time, which can eventually affect performance. Periodically, you should rebuild the table indexes and clean up the database row file and log file to ensure optimal database performance. In addition, there is an automated database cleanup utility, DBCLEANUP, that automatically runs periodically to maintain specific tables such as the audit log table to remove old entries. Appendix - Modifying Component Server Settings for information on setting the interval (Audit Log Cleanup Interval) to automatically run DBCLEANUP.

You can also run the DBCLEANUP command manually from the Manageability Server's Console tab in Platform Manager. To do this, follow the steps below:

1. Run the Platform Manager (refer Using the Intel® EMA Platform Manager Client Application for details).
2. From the navigation pane at left, select **Intel® EMA Servers > localhost > EMAManageabilityServer**.
3. Select the **Console** tab.
4. In the **Component Console** window, enter the command dbcleanup at the prompt and press Enter.

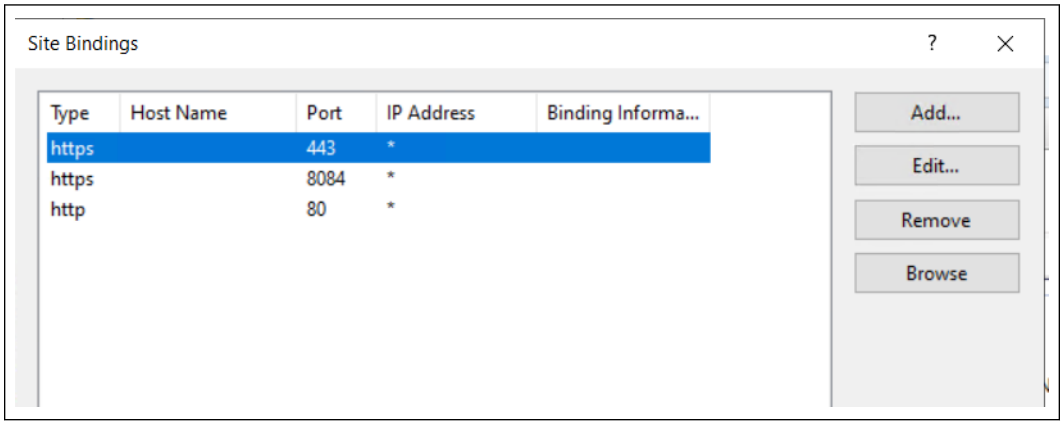
4.8 Restoring the Intel® EMA Server from Backup

In Security Recommendations section, we recommend that you back up your Intel® EMA database and MeshSettingsCertificate after installing Intel® EMA. This section describes how to restore your Intel® EMA server from that backup.

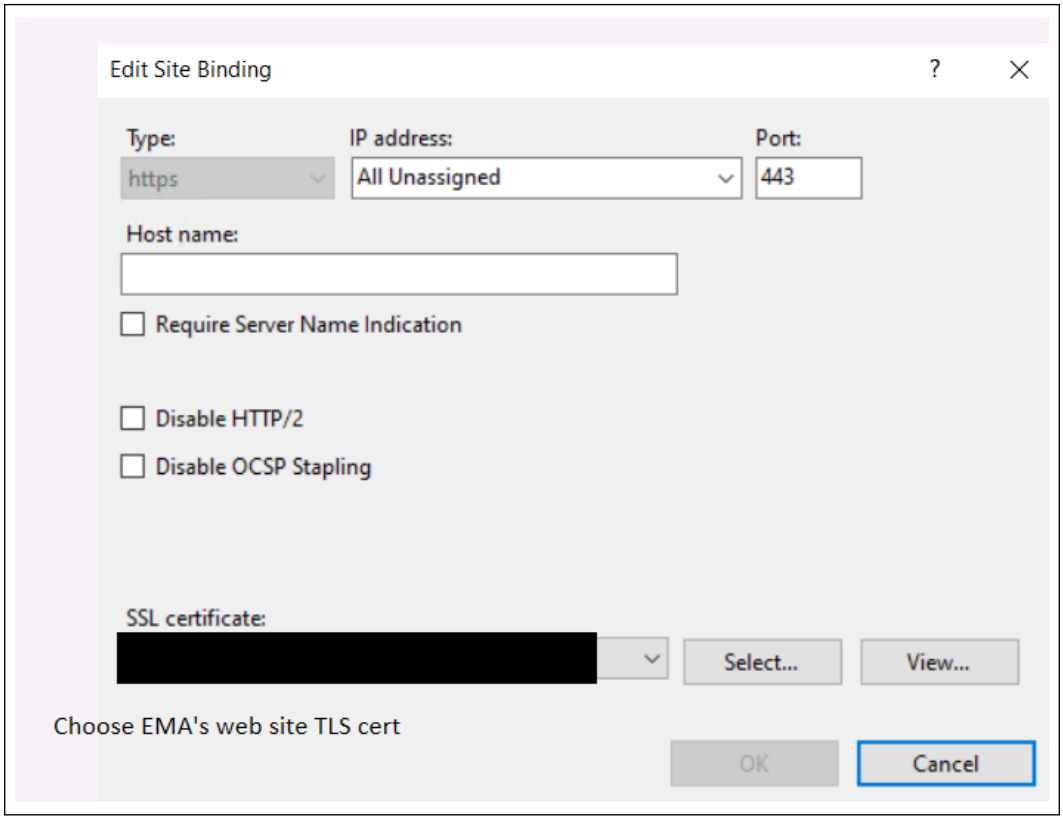
1. Start with a clean system.
2. Restore the database backup.
3. Restore the MeshSettingsCertificate certificate (including the private key) to the Local Machine/Personal location of the Certificate Store. The access of the private key needs to be open for the account running the Intel® EMA components and the account running Intel® EMA IIS website.

4. Run the Intel® EMA Installer and choose Single Server setup, as described in Installing or Updating the Intel® EMA Server on page 33. Be sure to point the installation to the restored database. The installer will indicate that you are performing an update installation. This is normal.
5. In IIS Manager, check to ensure IIS bindings are correct. You should see information similar to the following:

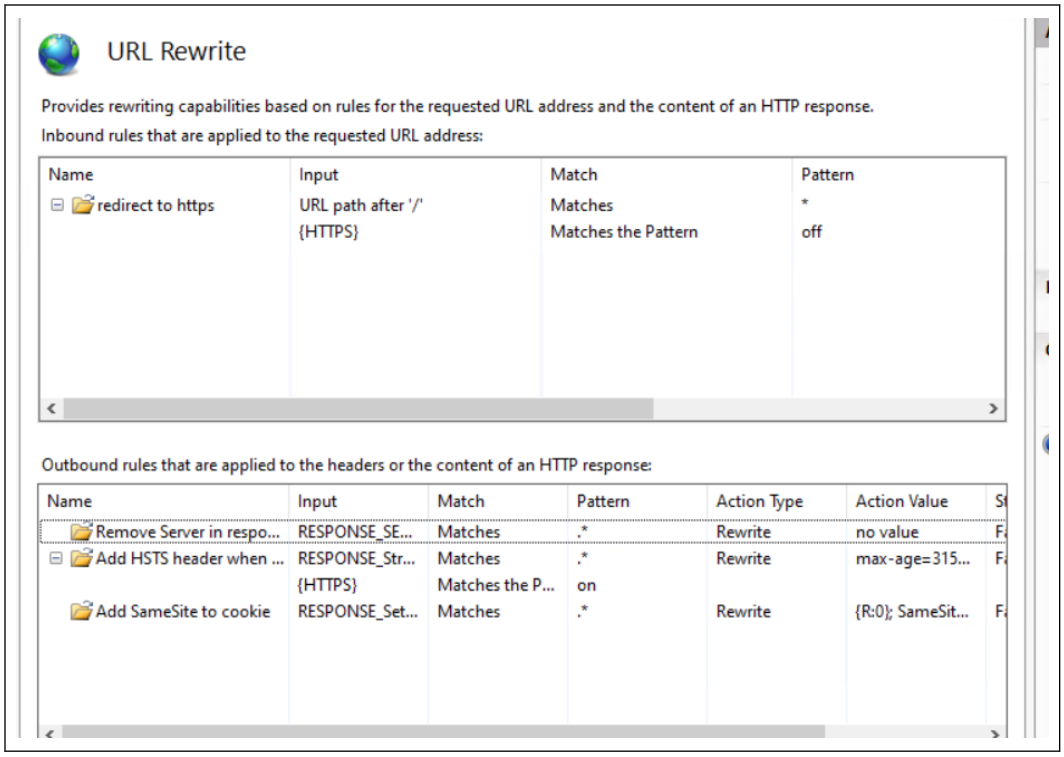
   Site bindings should be similar to this:



   For ports 443 and 8084, you should see binding details like this (with 443 or 8084 port):



   For URL rewrite, you should see settings like this:

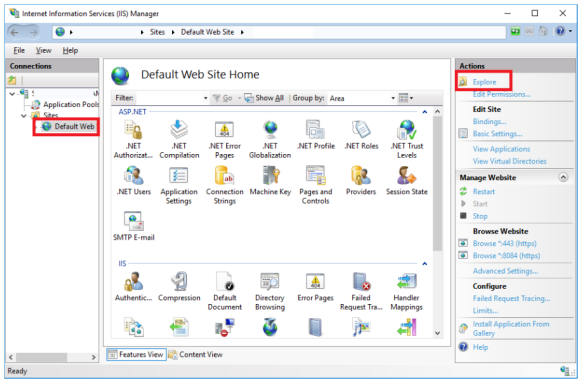
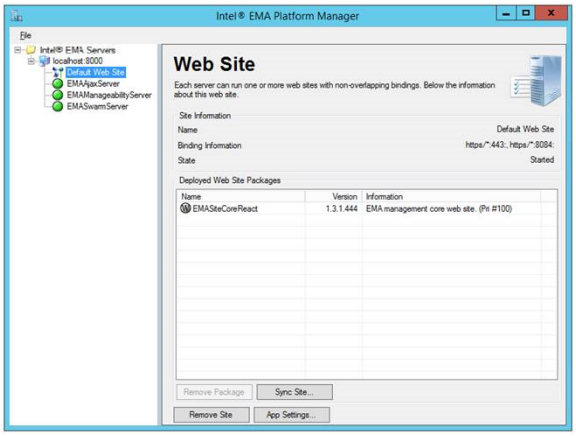

URL Rewrite
Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.
Inbound rules that are applied to the requested URL address:
Name
Input
Match
Pattern
redirect to https
URL path after '/'
Matches
*
{HTTPS}
Matches the Pattern
off
Outbound rules that are applied to the headers or the content of an HTTP response:
Name
Input
Match
Pattern
Action Type
Action Value
Remove Server in respo...
RESPONSE_SE...
Matches
.*
Rewrite
no value
Add HSTS header when ...
RESPONSE_Str...
Matches
.*
Rewrite
max-age=315...
{HTTPS}
Matches the P...
on
Add SameSite to cookie
RESPONSE_Set...
Matches
.*
Rewrite
{R:0}; SameSit...

5.0 Appendix: Troubleshooting After Installation

5.1 General Troubleshooting

Check logs, traces, or events	The installation log file EMALog-Intel®EMAInstaller.txt is located in the same folder as the Intel® EMA installer (i.e., wherever you downloaded and ran the installer). *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.` Refer Performing Intel® EMA Server Maintenance on page 74 for information on viewing the log file, trace file, or events for each of the Intel® EMA component servers.
Intel® EMA Server Installation Error	**Intel® EMA Platform Manager Package path not set correctly** The installer can find an existing Platform Manager settings file (e.g., C:\Program Files (x86)\Intel\Platform Manager \Platform Manager Server\settings.txt), but cannot find the Intel® EMA packages (e.g., C:\Program Files (x86)\Intel \Platform Manager\Packages) listed in that settings file. **To fix:** 1. Uninstall the Intel® EMA Server, selecting all options. 2. Ensure that Intel® EMA Platform Manger is no longer installed and there is no content in the Intel® EMA installation folder (e.g., C:\Program Files (x86)\Intel \Platform Manager). 3. Re-install the Intel® EMA Server.
Intel® EMA Platform Manager Service not starting	Like all Windows services, the Intel® EMA Platform Manager Service will timeout if the service takes too long to start (30 seconds by default). On slow machines, this timeout limit may be reached while the Intel® EMA Platform Manager Service is starting. If this happens Intel® EMA will not work correctly. Check the status, events, and log of this service: • In the **Windows Services** viewer, check to see if it is started successfully. • In the **Windows Event Viewer**, go to Windows Logs \ System and look for entries with Level: Error and Source: Service Control Manager. • If this service has exceptions thrown, you can find them in the log file, PlatformManagerError.txt, on your Windows drive (e.g. C:\PlatformManagerError.txt).

continued...

	To fix: Change the Windows registry settings to modify this timeout value. We recommend doing an internet search for "Error 1053 ServicesPipeTimeout" for information on how to do this.
Error when trying to access the Intel® EMA website	Ensure the website is deployed. The website may not be deployed due to the package path issue mentioned above. To fix: Use Windows IIS Manager to determine the folder of the Intel® EMA website (click **Explore** under **Actions**, top right). In that folder you should see many subfolders and files.  If not, use the Platform Manager to "sync site" and redeploy the website. 
The target Intel® EMA website URL must match the Intel® EMA website's certificate	If the URL used to access the Intel® EMA website does not match the Issued to field of Intel® EMA website certificate, the web browser's security filtering will block many features. **To fix:** Ensure Intel® EMA URL matches the **Issued to** field of the certificate.
Warnings and errors during Intel® AMT setup/provision	Depending on the target Intel® AMT firmware's status, some of the warnings/errors may be transient errors. The Intel® EMA Manageability server will automatically re-try the failed setup periodically. However, some of the warnings/errors are valid and need to be addressed.

continued...

	Note: Refer to the Platform Manager section of this guide for information on warnings and error messages logged by the Manageability server during the setup/provision process. Transient warnings/errors that can be ignored **Warning/Error type – OTP_REQUIRED:** Message:Host Based Admin Setup (1st try): OTP_REQUIRED Message:Unable to go to admin mode, rolling back out of client mode. **Warning/Error type – INTERNAL_ERROR due to Unauthorized WSMAN call:** Message:Creating DotNetWSManClient object... Warning:Error (2): Intel.Manageability.WSManagement.WSManException: The remote server returned an error: (401) Unauthorized. Message:Host Based Setup (1st try): INTERNAL_ERROR *Note:* The server will re-try the installation despite these errors until the third try. **Valid warnings/errors that must be addressed** PKI domain suffix not matching the PKI certificate: Warning/Error type – Message:Host Based Admin Setup (3rd try): AUTH_FAILED Warning/Error type – Message:Unable to go to admin mode, rolling back out of client mode. INTERNAL_ERROR due to Intel® Management and Security Application Local Manageability Service (LMS) not running correctly: Warning/Error type – Warning:Error (2): Intel.Manageability.WSManagement.WSManException: The underlying connection was closed: The connection was closed unexpectedly. Warning/Error type – Message:Host Based Setup (3rd try): INTERNAL_ERROR WSManException due to Intel AMT FW requiring a reset: Warning:Error (2): Intel.Manageability.WSManagement.WSManException: The underlying connection was closed: The connection was closed unexpectedly. ---> System.Net.WebException: The underlying connection was closed: The connection was closed unexpectedly. If this does not resolve after the Intel® Manageability Server retries the setup, then shut down the Intel® AMT machine, unplug the power cable and unplug the Ethernet cable to reset the Intel® ME firmware. Then reconnect the cables back and restart the machine. Error due to full certificate store in Intel® AMT FW: Error: .[omitted]….. Certificate Store in firmware is full and no more certificates can be added. In this case, we suggest to unprovision this Intel® AMT system. Then use Intel® EMA's manual provision or auto provision to set up this system again.
Intel® AMT operation does not work, but all other features function correctly	This section applies to the scenario where Intel® EMA server is installed under **Use hostname only** mode and the target endpoint is provisioned with Intel AMT CIRA. If Intel AMT operation does not work, but all other features work, it is very likely that the Intel AMT CIRA firmware cannot resolve the hostname/FQDN entered during Intel® EMA server installation. **To fix:** 1. Unprovision the target endpoint.

continued...

	2. With a clean setup and a clean/unprovisioned endpoint, perform a CIRA provision and monitor the provision events. a. To monitor, go to the EMAManageabilityServer's **Events** tab in Platform Manager. Make sure there are no errors (a few warnings are OK). b. On the target endpoint, open the **Intel® Management and Security Status Tool** and go to the **General** tab. If the provision is successful, you should see two events: **Configured** and **Remote Control Connection is Enabled**. c. If the provision was successful, continue with the remaining steps. Otherwise, check the event and logs of the Intel® Manageability server and fix the issues. 3. On the EMASwarmServer's **Component** tab (in Platform Manager), monitor the **ConIntelAmt** value. This is the number of active CIRA connections. If you provisioned one endpoint with CIRA and CIRA successfully established the connection to Intel® EMA Swarm server, this value should be 1. If this number is not correct, restart the target endpoint and wait for one to two minutes. If the **ConIntelAmt** value is still incorrect, continue with the remaining steps. 4. At this point, Intel AMT CIRA firmware probably cannot resolve the hostname/FQDN. To verify this, use the **fixed IP address** mode to do a provision. If fixed IP address mode works, then the root cause is due to the name resolution issue. In that case, consult your IT administrator. Follow these steps to temporarily use the **fixed IP address** mode: a. On the Server Settings page, change the ciraserver_ip setting of the Manageability server (refer Appendix - Modifying Component Server Settings on page 93). b. Save settings are restart the Manageability server. 5. Unprovision the target endpoint and re-perform the provision. This time, CIRA will use the IP address you specified above.
Uninstalling Intel® EMA server fails to drop the database	When uninstalling the Intel® EMA server, you may see the warning/error: "Unable to drop database." **To fix:** 1. Open Microsoft SQL Server Management Studio and connect to your database, then check the existing databases. Determine whether the Intel® EMA database is set to "Single User" mode. 2. Right click the target database and choose **Delete**. Do not change any default values in the Delete option window. Delete the target database. 3. If the database is not deleted, right-click the database server and choose **Restart**. After the database server is restarted, try to delete the target database again.
802.1x setup fails during Intel AMT provisioning -OR- Active Directory user validation fails after updating to v1.5.0 or later -OR- Active Directory option not available during installation or update to v1.5.0 or later	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

continued...

	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. Refer Appendix - Modifying Component Server Settings on page 93.
Intel® EMA agents fail to connect to server after updating to v1.4.0 or later	This may be due to disabled TLS cipher suites. As of v1.4.0, Intel® EMA restricted the usable TLS ciphers suites for the agent while leaving the older cipher used by Intel AMT enabled for CIRA. Check to ensure proper TLS cipher suites are enabled. Refer Disable Insecure Cipher Suites on page 21 and Strong Encryption Protocols on page 22 *Note:* This issue has been consistently observed in Windows Server 2022 installations due to default settings in the OS.
Error processing MeshSettingsCertificate during update installation	During an update installation, the installer will fail with an error message "Missing, invalid, or multiple MeshSettingsCertificates found" under the following circumstances: • No MeshSettingsCertificate was found in the Intel® EMA database • The MeshSettingsCertificate was found, but it is corrupted or in an invalid format • Multiple MeshSettingsCertificates were found in the Intel® EMA database **To fix:** To fix this problem, restore the last known good copy of the MeshSettingsCertificate to the Intel® EMA database from backup. Be sure to remove any invalid or additional copies of the certificate before restoring from backup. Refer Restoring the Intel® EMA Server from Backup on page 83 for information on restoring from backup.
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.
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. Starting with EMA version 1.14.x, a new HTTP TRACE verb was introduced, which can cause configuration conflicts. To resolve this issue: 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. To resolve this issue, ensure the Intel® EMA Agent is launched with administrator privileges using one of these methods: 1. Right-click method: Right-click the EMA Agent executable and select "Run as administrator" 2. Command line method: Open Command Prompt as administrator and launch the agent from the command line.

continued...

	Running the agent without administrator privileges will prevent the KVM session from displaying properly, resulting in a blank screen during remote console access.
Endpoints not connecting after update to Intel® EMA1.15.0	After updating to Intel® EMA 1.15.0, endpoints in new endpoint groups or Intel® AMT systems provisioned after the update may fail to connect to the server. Verify that your firewall rules include port 8081. Refer to Network Ports in section 1.3.11 for the full list of required open ports.

5.2 Distributed Server Installation Troubleshooting

Server components (Swarm, Ajax, etc.) do not appear to be connecting to each other across machines 9	Check the following: • **Load Balancer:** Ensure your load balancer is configured properly per its documentation. Specifically, ensure that health checking rules and traffic forwarding rules include ports 443 (front-end), 8084 (front-end), 8080, and 8081 (agent and Intel AMT CIRA connections). For ports 443 and 8084, traffic forwarding rules must have session persistence (stickiness) enable. • Firewall and Network Ports: Ensure your firewall rules have the required ports set to Open. Refer Installation Prerequisites on page 12 "Server network ports" . Also check any other network security rules for your environment. • **Server Settings:** On the Server Settings page of the Intel® EMA UI, check the following for each component server: — **Server IP addresses:** ensure the correct list of IP addresses is shown for each type of component server. — **Message Port: T**his is the port that this component server type is listening on for inter-component messages. If you changed this in Server Settings, make sure the new port is not blocked by a firewall. — **Swarm Server list:** Ensure the correct list of "[Machine ID]:[Machine IP Address]" pairs for the Swarm Servers in your distributed installation. You can verify the Machine ID in the Intel® EMA database under the Server Settings table. Then use the Machine Name to obtain the correct IP Address for that machine. — After verifying, test the components by starting Platform Manager and running "testmessage" on the Console tab of one of the Intel® EMA components. Each component should be able to send out a blast message to all other components (including itself) on all machines in the distributed installation. Verify the reception of the messages in the Events tab of each component on each machine.
Authentication fails intermittently	Ensure that all Intel® EMA websites in the distributed environment are using the same machine keys. Verify this using IIS Manager on each machine where the Intel® EMA website is hosted. Refer Summary on page 58
From one of the machines in a distributed server architecture installation: • Platform Manager client cannot connect to the Platform Manager service -OR- • Cannot open the Intel® EMA UI in a browser	In a distributed environment, if you install Intel® EMA under Kerberos (Windows Authentication), the Platform Manager client may have difficulty connecting to the Platform Manager service from one of the distributed server machines. Similarly, you may have difficulty opening the Intel® EMA UI in a browser from one of the distributed server machines.

continued...

	This is due to the Service Principal Name (SPN) for the load balancer not being configured correctly in Active Directory. **To fix:** To fix this problem, ensure your SPN for the load balancer is correctly configured. Also, you can use one of the other server machines' FQDN for the target URL, not the load balancer's FQDN (the other machine must have an Ajax or Web server installed). Doing so will allow you to launch Platform Manager or browse to the Intel® EMA website from one of the server machines in your distributed environment (i.e., a host managed by the load balancer), regardless of the SPN configuration for the load balancer. *Note:* From all other machines (i.e., systems not managed by the load balancer), you can simply use the load balancer's FQDN.
Endpoints not connecting after update to Intel® EMA1.15.0	After updating to Intel® EMA 1.15.0, endpoints in new endpoint groups or Intel® AMT systems provisioned after the update may fail to connect to the server. Verify that your load balancer is configured to forward port 8081 in addition to port 8080 for agent and Intel® AMT CIRA connections.

6.0 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.

6.1 Swarm Server

Setting	Description
UI: Admin Port **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 **API: adminportlocal**	Determines if the Admin TCP listener will only bind to the local loopback or not. Values are 0 and 1. 0 = Distributed-server environment 1 = Single server environment
UI: Agent Auto Update **API: enableAgentAutoUpdate**	Boolean. Enables or disables automatic agent update. Default: Enabled.
UI: Agent Update Interval (Seconds) **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. Default: 10. Minimum: 10. Maximum: 120.
UI: Log File Path **API: logfilepath**	Path to the Intel® EMA logfile. Maximum: 247 characters Minimum: 2 characters
UI: Enable Intel CIRA Power State Polling **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 **API: maxdbconnections**	The maximum number of concurrent DB connections for this server.
UI: Swarm Servers **API: swarmserver**	List of active Swarm Servers. Includes Server ID and Server IP & Port (format IP Address: port).
UI: Server Ips **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 **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 **API: tcpConnRetrySeconds**	Wait time between retries when establishing communication connections between Intel® EMA server components.
UI: TCP Connection Idle **API: tcpConnIdleSeconds**	Interval between heartbeat messages sent between components once communications are established.
UI: Database Connection Wait Time (Minutes) **API: dbConnectionWaitTimeMinutes**	Amount of time in minutes that Intel® EMA will wait for getting a database connection. Range: 1 - 10 Default: 2
UI: Database Lock Timeout Period (Seconds) **API: dbSetLockTimeoutSeconds**	Amount of time in seconds that a SQL query will keep a lock. Range: 1 - 60 Default: 2
UI: Database Retry Hold Time for a Query (Milliseconds) **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. Range: 100 - 60000 Default: 100
UI: Database Retry Attempts for a Query **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. Range: 3 - 100 Default: 5
UI: CIRA Keep-alive Interval (Seconds) **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. Default: 10 seconds Min: 10 seconds Max: 1 hour (i.e., 3,600 seconds)

6.2 Ajax Server

Setting	Description
UI: Ajax Cookie Auto Refresh Range **API: ajaxCookieAutoRefreshRange**	Range in minutes in which the Ajax cookie life can be extended.
UI: Ajax Cookie Idle Timeout **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 **API: httpheader_Access-Control-Allow-Headers**	Additional headers to set in response to the Ajax request.
UI: Log File Path **API: logfilepath**	Path to the Intel® EMA logfile. Maximum: 247 characters Minimum: 2 characters
UI: User Access Failed Max Count **API: userAccessFailedMaxCount**	Number of failed password attempts before user account is locked by the Web API.
UI: Expire Sessions **API: expiresessions**	Sets whether the Ajax server should expire the session or not (default is enabled).
UI: Maximum Number of Concurrent Database Connections **API: maxdbconnections**	The maximum number of concurrent DB connections for this server.
UI: Server IPs **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 **API: swarmserver**	List of active Swarm Servers. Includes Server ID and Server IP & Port (format IP Address: port).
UI: Message Port **API: messagePort**	The TCP port this component server type is listening on to accept internal traffic from other Intel® EMA components. Default 8092.

6.3 Manageability Server

Setting	Description
UI: CIRA Server Host **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 **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 **API: logfilepath**	Path to the Intel® EMA logfile. Maximum: 247 characters Minimum: 2 characters
UI: Maximum Number of Concurrent Database Connections **API: maxdbconnections**	The maximum number of concurrent database connections for this server.
UI: USBR Images Root Directory **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**. *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 **API: maxUsbrImageStorageCapacityPerTenantInGigabytes**	Disk space in GB each tenant is allowed for USBR image storage. Default: 20 GB Maximum: 50 GB
UI: Maximum USBR Image storage Capacity Per EMA Instance **API: maxUsbrImageStorageCapacityPerEmaInstanceInGigabytes**	Total disk space in GB (for all tenants) allowed in this Intel® EMA instance for USBR image storage. Default: 50 GB Maximum: 500 GB
UI: Maximum USBR Slot Count per Tenant **API: maxUsbrSlotCountPerTenant**	Number of active USBR sessions allowed for each tenant.
UI: Maximum USBR Idle time **API: maxUsbrIdleTimeInMinutes**	Length of time in minutes a USBR session can be idle before being automatically terminated.
UI: USBR Redirection Manager Loop Interval **API: usbrRedirectionManagerLoopIntervalInSeconds**	Status polling interval in seconds for active USBR sessions.
UI: USBR Redirection Throttling Rate **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. *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. Default value: 0, max value 1000, min value 0. Suggested value = start at 10, increment by 10 to find appropriate rate for your network.
UI: File Upload Retention Period **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 **API: fileUploadCleanupIntervalInHours**	Interval in hours that file cleanup process would run to process incomplete resumable files.
UI: Swarm Servers **API: swarmserver**	List of active Swarm Servers. Includes Server ID and Server IP & Port (format IP Address: port).
UI: Server IPs **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 **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) **API: AuditLogCleanupIntervalInHours**	Interval in hours before cleanup of audit log records in the Intel® EMA database.
UI: Audit Log Retention Period (Days) **API: AuditLogRetentionPeriodInDays**	Interval in days before cleanup of audit log records in the Intel® EMA database.
UI: Enable 8021X Certificate Auto Renewal **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) **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. Default: 30 Maximum: 90 Minimum: 1
UI: Enable Provisioning TLS Certificate Revocation Check **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. Default: True.

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

continued...

Settings	Description
UI: Swarm Server Host **API: SwarmServerHost**	Hostname or IP address of the Swarm server, or the load balancer of the Swarm servers.
UI: Swarm Server LegacyPort **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 **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 **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. Refer the note for LDAP Connection Port below.
UI: LDAP Connection Port **API: LdapConnectionPort**	The port used for LDAP connection in 802.1x configuration. Default port is secure 636. *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 **API: MaxAccesstokenTTL**	Maximum time for API bearer tokens to be refreshed.
UI: Frontend Storage Type **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 **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 **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 **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 **API: SamlIdpEntityId**	The SAML IDP Entity ID Value, only used when SAML authentication option is selected. 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 Entity ID is case-sensitive *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 **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) Obtain the App Federation Metadata URL from your IdP. Import this metadata into your application's SAML configuration settings. The EMA sever will try to connect to the provided URL to check its validity, make sure the URL reachable before changing this setting. Only HTTP and HTTPS schemes are supported. *Note:* When changing this setting you need to recycle the IIS Appool, reset the website or webserver running the EMA WebSite.

6.5 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. Default: true.

continued...

Settings	Description
API: enableUnauthTcpConnectionIdleTimeout	
UI: TCP connection timeout 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. Default: 10000 Maximum: 3,600,000 (1 hour)
UI: Rate Limiter 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. Default: true.
UI: Rate Limiter Window Size API: rateLimiterWinSizeInMilliSeconds	The window size in milliseconds to use for tracking requests with per-IP address rate limiting. Default: 200 Maximum: 3,600,000 (1 hour)
UI: Ajax HTTP Requests Max Count 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). Default: 20 Maximum: 1,000,000
UI: Recovery HTTP Requests Max Count 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). Default: 20 Maximum: 1,000,000
UI: Message Ports Requests Max Count (Before Authorization) 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). Default: 100 Maximum: 1,000,000
UI: Message Ports Requests Max Count (After Authorization) 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). Default: 80,000 Maximum: 1,000,000
UI: Swarm Admin Ports Request Max Count (Before Authorization) 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). Default: 20,000 Maximum: 1,000,000
UI: Swarm Admin Ports Request Max Count (After Authorization) 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). Default: 20,000 Maximum: 1,000,000
UI: Agent Port Request Max Count (Before Authorization) 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). Default: 20 Maximum: 1,000,000

continued...

Settings	Description
UI: Agent Port Request Max Count (After Authorization) 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). Default: 1000 Maximum: 1,000,000
UI: Connection Count Check API: enableConnectionCountChecker	Boolean. When enabled Intel® EMA will limit the TCP TLS connection count per-IP address to help prevent Denial of Service attacks. Default: true.
UI: Message Port (connections per port) API: blastMessageConnCountChecker	The maximum number of connections per-IP address allowed to the internal component-to-component ports (8092, 8093, 8094). Default: 20 Maximum: 1,000,000
UI: Admin Port (connections per port) API: swarmAdminPortConnCountCheck er	The maximum number of connections per-IP address allowed to the Swarm Server Admin port (8089). Default: 20,000 Maximum: 1,000,000
UI: Swarm Agent Port (connections per port) API: swarmAgentPortConnCountChecker	The maximum number of connections per-IP address allowed to the Swarm Server Agent port (8080, 8081) . Default: 20,000 Maximum: 1,000,000
UI: User password minimum length API: userPasswordMinLength	Used to customize policy for password validation. Default: 8 Minimum: 8 Maximum: 20
UI: User password maximum length API: userPasswordMaxLength	Used to customize policy for password validation. Default: 255 Minimum: 64 Maximum: 255
UI: Client Credentials minimum length API: clientCredentialsMinLength	Used to customize policy for password validation. Default: 12 Minimum: 12 Maximum: 20
UI: Client Credentials maximum length API: clientCredentialsMaxLength	Used to customize policy for password validation. Default: 255 Minimum: 64 Maximum: 255
UI: Complexity required (uppercase/lowercase/special char) API: passwordComplexityRequired	Used to customize policy for password validation.True/False. Default: True
UI: Password Disallowed List Checking 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. Default: True.
UI: 2FA TOTP Algorithm API: MfaTotpAlgorithm	Used to indicate the algorithm used by MFA TOTP. 0 means SHA1, 1 means SHA256, and 2 means SHA512. Default: 0 Minimum: 0 Maximum: 2

6.6 Recovery Server Settings

The settings below are provided to support future Intel platforms.

Settings	Description
UI: Log File Path API: logfilepath	Path to the Intel® EMA logfile. Maximum: 247 characters Minimum: 2 characters
UI: Maximum Number of Concurrent Database Connections API: maxdbconnections	The maximum number of concurrent database connections for this server.
UI: Message Port 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 API: RecoveryPort	Port to be used for recovery. Default 8085. *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 API: RecoveryPortEnabled	Boolean, default "True." Specifies whether or not the recovery port is enabled.
UI: Server IPs 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.

7.0 Appendix – Domain/Windows Authentication Setup

The Intel® EMA installer sets up the fundamental settings for domain/Windows authentication if it is installed under domain/Windows authentication mode. However, there are many different network infrastructure scenarios. Some of the scenarios require the IT administrators to perform extra steps.

7.1 Server Connection Information Set at Installation

While running the Intel® EMA installer, at the hostname field of External Identity setup, we suggest using the NetBIOS hostname or NetBIOS FQDN of your machine in the Hostname field. You still need to make sure that other endpoints or other client web browsers can connect to the value you entered here. You can find your NetBIOS name by right-clicking **This PC** in Windows File Explorer, and choosing Properties.

If you decide to use another value (e.g., in a load balancing scenario), follow IT practice to set up the Service Principle Name (SPN) after Intel® EMA is installed.

7.2 IIS Website's Authentication and .NET Authorization

Intel® EMA sets the following properties (differently from most default IIS website setups) for the Intel® EMA website when it is installed under domain/Windows authentication mode:

- At IIS \ Authentication, also enable "Anonymous Authentication" with "Application Pool Identity"
- At ASP.NET \ .NET Authorization Rules, "Anonymous Users" need to be allowed

Double check that these properties are set correctly.

7.3 Optional – Grant Permission to Website Content

There are several options for setting up this permission, e.g., NTFS or URL Authorization. IT administrators need to set it up based on their specific infrastructure need.

7.4 Optional – Double-hop Structure

In a normal Intel® EMA installation, you don't need to do this. However, if you need to support special double-hop authentication, e.g., passing the logged-in credential to another backend server, then you need to set up several extra settings, e.g., **Delegation** at AD's Computer object for your server machine. Please follow standard IT practice.

7.5 References

- https://blogs.msdn.microsoft.com/webtopics/2009/01/19/service-principal-name-spn-checklist-for-kerberos-authentication-with-iis-7-07-5/
- https://weblogs.asp.net/owscott/iis-using-windows-authentication-with-minimal-permissions-granted-to-disk
- https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/authentication/anonymousauthentication
- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831722(v=ws.11)

8.0 Appendix – Configuring 802.1X for Active Directory

This section is intended for Intel® EMA Global Administrators who want to enable 802.1X authentication for Intel® AMT. If your Tenant Administrators plan to configure 802.1x profiles for use in their Tenant-specific Intel AMT profiles, the Global Administrator must configure 802.1x for Active Directory Domain Services, specifically an Active Directory Organizational Unit (OU) and Active Directory Certificate Service certificate template, as described in this section. Note that the configuration described here is just one possible configuration. Those highly familiar with 802.1x configuration may wish to deviate from this configuration.

Intel® EMA supports Extensible Authentication Protocol (EAP).

NOTE

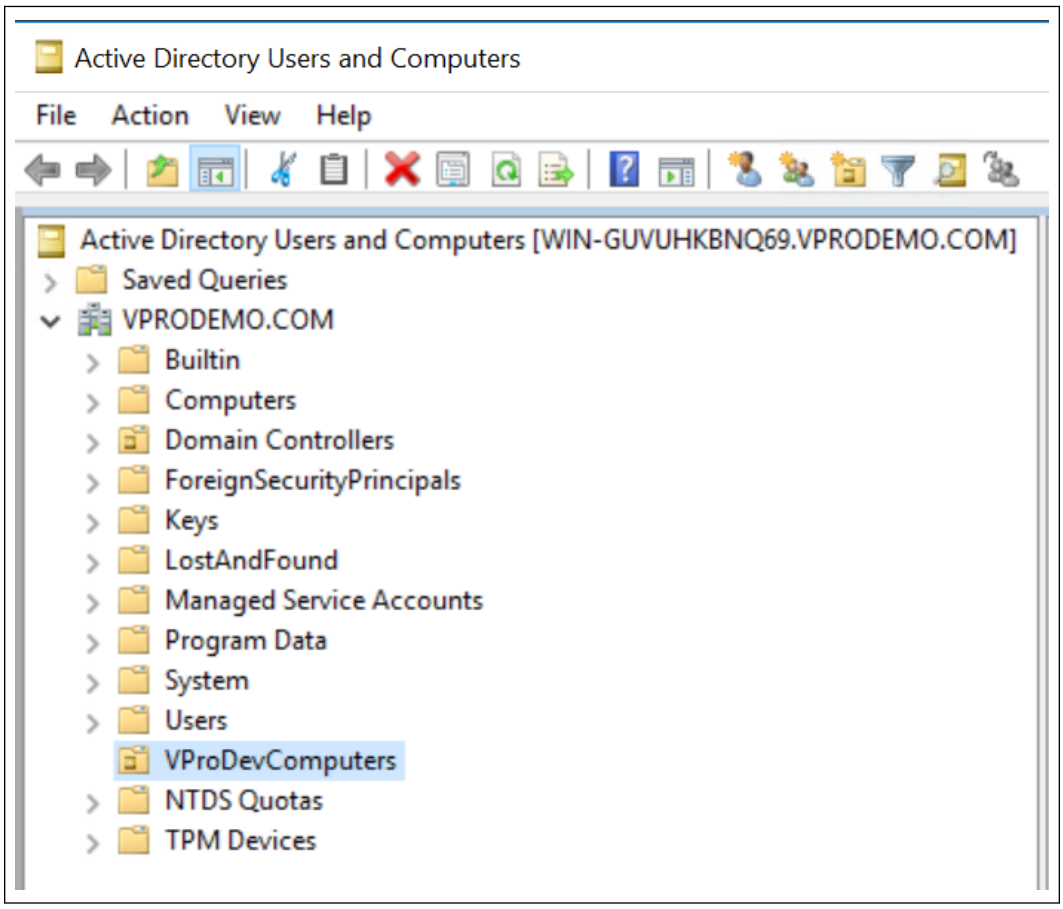
This section focuses on configuration for the Intel® EMA server system to enable 802.1x authentication at the overall server level as a prerequisite for configuring 802.1x profiles for a specific Tenant in Intel® EMA. For information on configuring an 802.1x profile for a specific Tenant usage space, Refer Intel® EMA Administration and Usage Guide

8.1 Active Directory Domain Services

During Intel AMT configuration of an endpoint, Intel® EMA creates an Intel AMT computer object (identified by -iME suffix) within the AD OU as defined in the 802.1x profile. This object is used by Intel AMT to support Kerberos authentication. Note that the AD OU requires full permissions for the user account running the Intel® EMA Manageability Server. Follow the steps below to create an AD OU for this purpose.

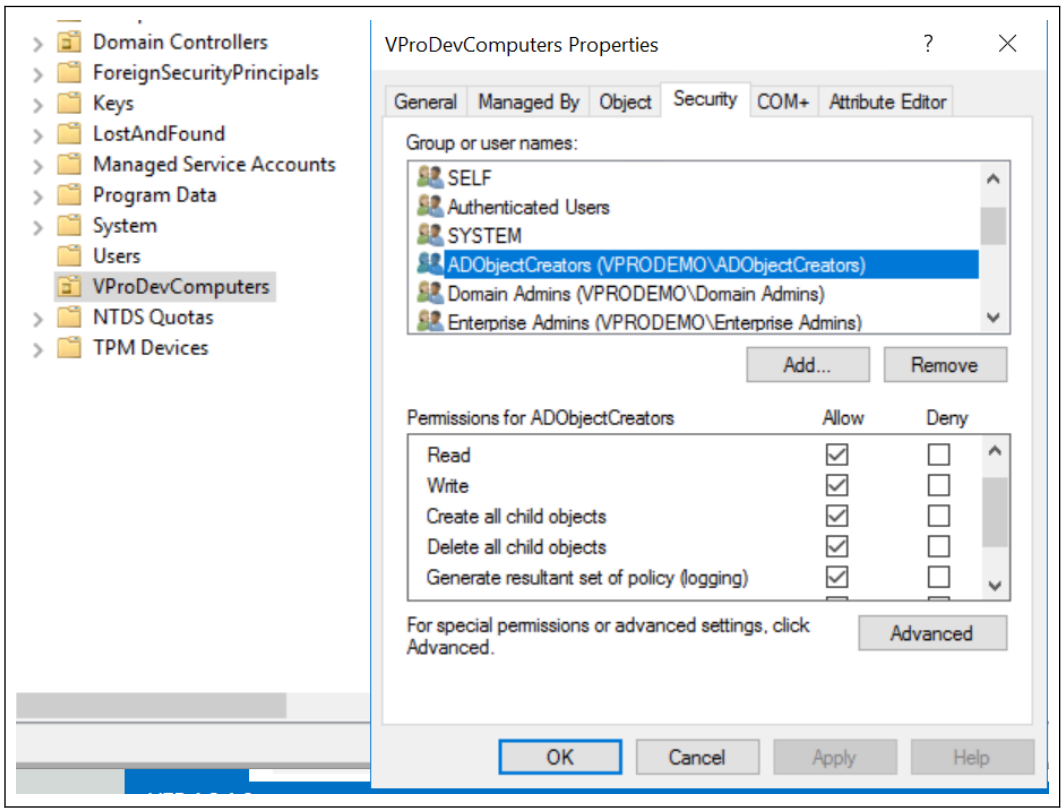
1. Add an Organization Unit to the AD Domain to which the endpoint belongs. The example below uses the domain **VPRODEMO.COM** and the Organizational Unit, **VProDevComputers**.

Figure 2. Add New Organization Unit



2. Add privileges for the Intel® EMA server user account.
   a. Add the user account or a security group to which the user account belongs to the Security tab of the Organizational Unit where the AD Computer objects for 802.1X authentication will be created. Ensure that this account or security group has all available permissions allowed, and edit the Advanced Security Settings to apply this group's privileges to "This object and all descendant objects."

Figure 3. Modify Security List of the Org Unit



8.2 Active Directory Certificate Services

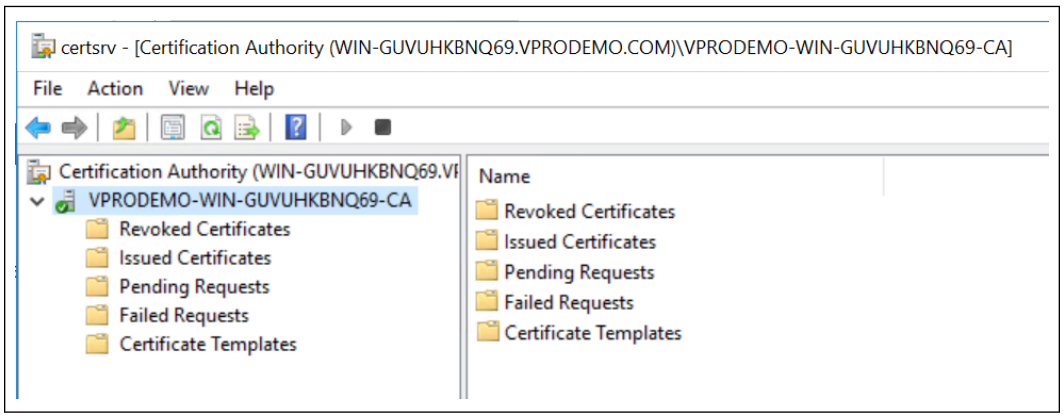
NOTE

This section is not required for EAP_PEAP_MSCHAP_V2.

EAP-TLS mandates that a Client Authentication and Trusted Root certificates are required. The Intel AMT 802.1x client certificate requires an Active Directory Certificate Service certificate. A duplicate of the Workstation authentication template with the specific properties described in step 2 below can be used.

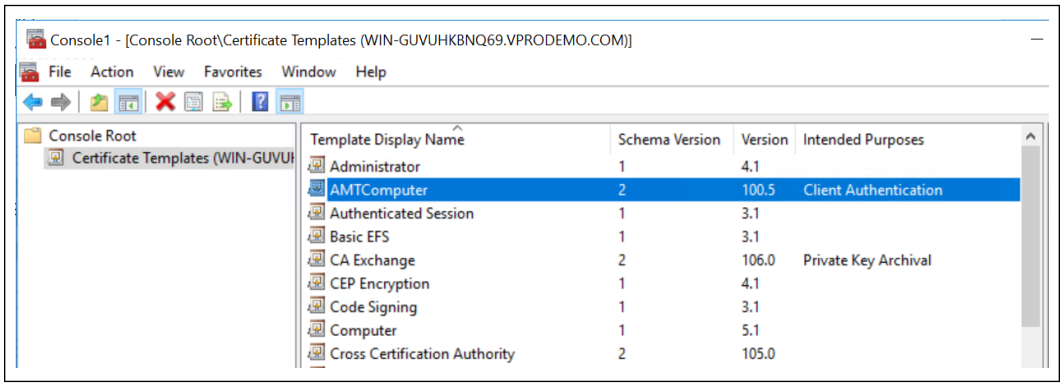
1. Choose the Certification Authority (Enterprise root CA) that is associated with your specific 802.1x environment configuration; the example below uses VPRODEMO-WIN-GUVUHKBNQ69-CA.

Figure 4. Cert Authorization List



2. Create a Certificate Template: **AMTComputer**. This is a duplicate template based on the Workstation Authentication template.

Figure 5. Certificate Templates list



a. Right-click **AMTComputer** and select **Properties**.

b. On the Subject Name tab, select **Supply in the request**.

c. On the Request Handling tab, if you plan to use the Microsoft Certificate Authority for certificate configuration under Client Authentication in your 802.1x profile (recommended, refer Intel® EMA Administration and Usage Guide), leave the box **Allow private key to be exported** unselected (recommended). If you plan to select "From Database" instead of Microsoft Certificate Authority in your 802.1x profile, then select this checkbox.

d. On the security tab, grant **Read** and **Enroll** permissions to any system (AD computer) running an Intel® EMA server instance.

e. Enable the template in the Certification Authority (right-click on Certificate Template and select **New > Certificate Template to Issue**).

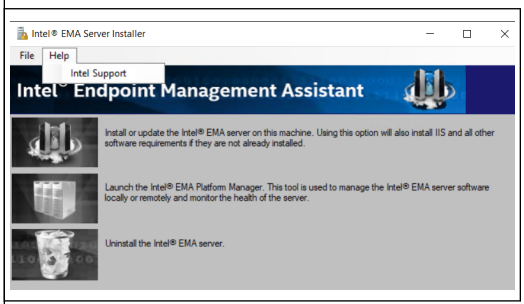
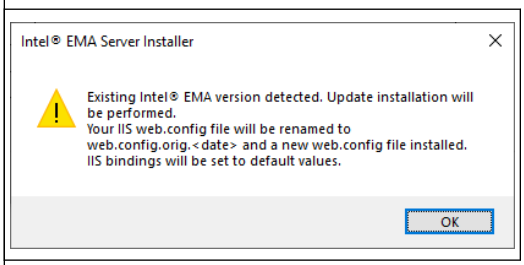
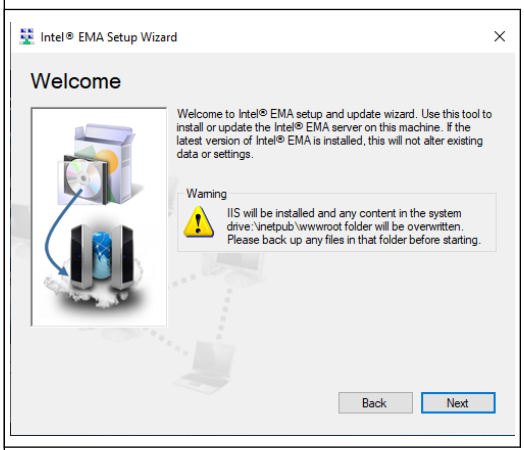
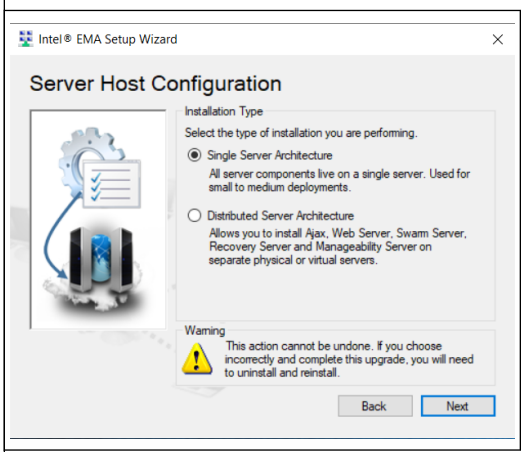
9.0 Appendix - Updating a Single Server Architecture Environment

If you are updating an existing Single Server Architecture installation of Intel® EMA, follow the procedures in this appendix.

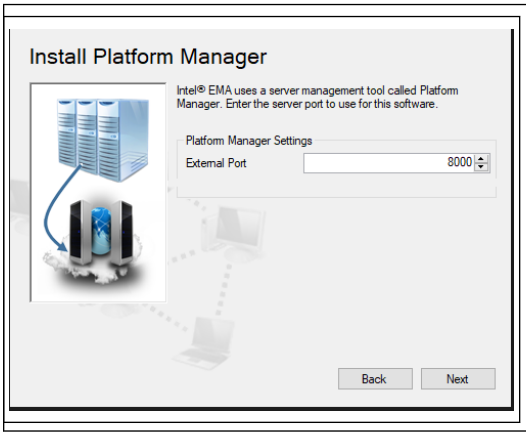
NOTES

- When upgrading an Intel® EMA instance, the account under which the Platform Manager service runs reverts to Local System. If you are running that service under another local or domain account, it will need to be reconfigured and all Intel® EMA components halted and restarted after the upgrade is complete.
- If you are updating from an existing version of Intel® EMA, the Intel® EMA website's bindings in IIS will be set to default values during the update installation. You can check the log files after installation to find the pre-update bindings for your reference.
- The Intel® EMA Agent software on managed endpoints is automatically updated upon connecting to the updated Intel® EMA server instance for the first time after server update. For Intel® EMA version 1.5.0 and later, this automatic update is only performed if the Swarm Server setting Agent Auto Update is enabled (default). Refer section below for more details.
- For updates from previous Intel® EMA versions, the installer detects the connection string automatically.

9.1 Updating Using the Setup Wizard

	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**
	The installer detects that you are performing an update installation and informs you that your IIS web.config file will be renamed to allow an updated file to be installed. Click **OK**.
	Click **Next** on the Welcome screen to continue the setup process. *Note:* The warning regarding IIS being installed does not apply to update installations.
	Select **Single Server Architecture**. This screen is only displayed if you are updating from a version prior to v1.6.0. *Important:* Selecting an installation type that does not match your existing installation will result in a non-functioning Intel® EMA instance that will need to be fully uninstalled and reinstalled. Make sure the type you select matches the type that is currently installed. **This action cannot be undone once you complete the update**. Click **Next**.

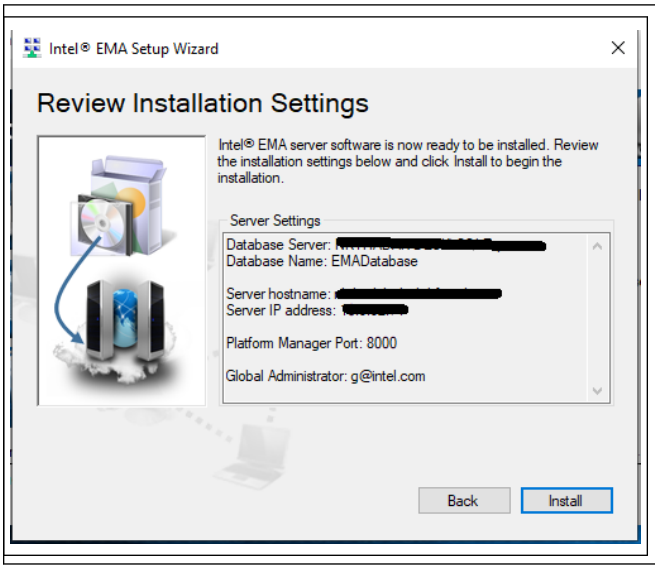
9.1.1 Platform Manager Configuration



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.

9.1.2 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.

9.2 Updating Using the Command Line

Use the command example below to update the Intel® EMA server machine.

```
EMAServerInstaller FULLINSTALL --updateinstalltype=single --
accepteula -c -v
```