



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

## **Single Server Installation Guide**

---

**Intel® EMA Version: 1.5.1**

**Document update date: Wednesday, August 18, 2021**

## Legal Disclaimer

Copyright 2018-2021 Intel Corporation.

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

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

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

No product or component can be absolutely secure.

Your costs and results may vary.

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

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

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

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses. Check with your system manufacturer or retailer or learn more at <http://www.intel.com/technology/vpro>.

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

---

<b>1 Introduction</b>	<b>1</b>
1.1 Before You Begin	1
1.2 Supported Operating Systems	2
1.3 Installation Prerequisites	2
1.4 Security Recommendations	5
1.4.1 Back Up Important Data	5
1.4.2 Modify the Access Control List (ACL) for Key Configuration Files	6
1.4.3 Enable Transparent Data Encryption on SQL Server Enterprise	6
1.4.4 Secure all Certificates and Keys	6
1.4.5 Samples files for Intel® EMA REST API and JavaScript library	6
1.4.6 Disable Insecure Cipher Suites	6
1.4.7 Strong Encryption Protocols	7
1.4.8 IIS – Replace the Temporary Web TLS Certificate	7
1.4.9 IIS – Change IIS User Account	8
1.4.10 IIS – Enabling the Transport Layer Security Protocol	9
1.4.11 IIS – Machine Key Validation Method	9
1.4.12 IIS – Restrict Unlisted IIS Extensions Execution	9
1.4.13 IIS – Dynamic IP Address Restrictions	9
1.4.14 IIS – Configure Host Headers for All Sites	9
1.4.15 IIS - Review updated web.config File	9
1.4.16 Check Binary Signatures	10
1.4.17 Change the Platform Manager Service User Account	10
1.4.18 Modify permissions of SQL Server user if desired	11
1.4.19 User Creation and Management	11
1.4.20 Use SQL Server Installed with TLS	12
1.5 Intel® EMA Installed Components	12
1.6 Important File and Directory Locations	13
1.7 Scaling Considerations	13
<b>2 Installing or Updating the Intel® EMA Server</b>	<b>15</b>
2.1 Installing Using the Setup Wizard	16
2.1.1 Server Host Configuration	16
2.1.2 Database Settings	17
2.1.3 Server Host Information	18
2.1.4 Platform Manager Configuration	18
2.1.5 User Authentication	18

---

2.1.5.1 Normal Accounts .....	19
2.1.5.2 Domain Authentication .....	19
2.1.6 Global Administrator Account Setup .....	20
2.1.7 Summary .....	20
2.2 Performing an Update Installation Using the Setup Wizard .....	21
2.2.1 Database Settings .....	22
2.2.2 Platform Manager Configuration .....	23
2.2.3 Summary .....	23
2.3 Installing or Updating Using the Command Line .....	23
2.3.1 Basic Mode .....	24
2.3.2 Advanced Mode .....	25
2.3.3 Performing an Update Installation Using the Command Line .....	25
2.4 Uninstalling .....	25
2.4.1 Uninstalling Using the Installer GUI .....	26
2.4.2 Uninstalling Using the Command Line .....	26
2.5 Intel® EMA Installer Advanced Mode Menu Bar .....	26
<b>3 Using the Global Administrator Interface .....</b>	<b>28</b>
3.1 Changing the Global Administrator Password .....	28
3.2 Creating and Deleting Tenants .....	28
3.3 Managing Users and User Groups .....	28
3.3.1 Adding, Modifying, and Deleting User Groups .....	28
3.3.2 Adding, Modifying, and Deleting Users .....	29
<b>4 Performing Intel® EMA Server Maintenance .....</b>	<b>30</b>
4.1 Manually Installing Platform Manager .....	30
4.2 Configuring the Intel® EMA Platform Manager Service .....	30
4.2.1 Platform Manager TLS Certificate .....	30
4.2.2 Mutual TLS Certificate for Client Authentication .....	30
4.3 Using the Intel® EMA Platform Manager Client Application .....	31
4.3.1 Starting Intel EMA Platform Manager .....	31
4.3.2 Monitoring Component Server Events .....	31
4.3.3 Monitoring Component Server Internal Tracking Information .....	32
4.3.4 Performing Basic Controls on Component Servers .....	32
4.4 Deploying New Packages .....	35
4.5 Updating the Database Connection String .....	35
4.6 Periodic Database Maintenance .....	36

---

4.7 Restoring the Intel® EMA Server from Backup .....	36
<b>5 Appendix: Troubleshooting After Installation .....</b>	<b>38</b>
<b>6 Appendix – Modifying Component Server Settings .....</b>	<b>44</b>
6.1 Swarm Server .....	44
6.2 Ajax Server .....	45
6.3 Manageability Server .....	46
6.4 Web Server .....	48
6.5 Security Settings .....	49
<b>7 Appendix – Domain/Windows Authentication Setup .....</b>	<b>52</b>
7.1 Server Connection Information Set at Installation .....	52
7.2 IIS Website's Authentication and .NET Authorization .....	52
7.3 Internet Explorer Used by the End User .....	52
7.4 Optional – Grant Permission to Website Content .....	52
7.5 Optional – Double-hop Structure .....	52
7.6 References .....	53
<b>8 Appendix – Configuring Network Infrastructure for 802.1X Authentication .....</b>	<b>54</b>
8.1 RADIUS Server - NPS .....	54
8.2 Configure a Microsoft NPS .....	55
8.2.1 Dependencies .....	55
8.2.2 Step 1 – Adding the NPS Role to Windows Server .....	55
8.2.3 Step 2 – Configuring NPS as a RADIUS Server .....	56
8.2.4 Post-configuration Actions .....	57
8.2.4.1 Create or edit a RADIUS client .....	57
8.2.4.2 Create or edit a Connection Request Policy .....	58
8.2.4.3 Create or edit a Network Policy .....	58
8.3 Configuring the RADIUS Clients .....	59
8.4 Connecting Endpoints to the Network .....	60
8.5 Environment Setup Example .....	60
8.5.1 Active Directory Domain Services .....	61
8.5.2 Active Directory Certificate Services .....	65
8.5.3 Network Policy Server .....	65
8.5.4 Wired Connection .....	68
8.5.5 Wireless Connection .....	70
8.6 Glossary .....	70

# 1 Introduction

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

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

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

This document 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 Section 2. 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 Section 1.3, are met.
- Review the Security Recommendations in Section 1.4 and implement them as part of or after installing Intel EMA.
- Review the Scaling Considerations in Section 1.7 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 whether you plan to install Intel EMA under domain authentication mode (Kerberos) or normal account (username/password) mode, the default. If 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.
- If you are installing or updating to version 1.5.0 of Intel EMA using Active Directory (AD), and you have configured AD to use non-default ports, you may experience issues installing and using Intel EMA. You can use the Intel EMA API **POST /api/latest/accessTokens/getUsingWindowsCredentials** to verify the current AD username/password with Active Directory (see the "AccessToken.htm" "Authentication" block in the sample code included with the installation package). If this API fails, either enable LDAPS secure port 3269 (recommended) or change the Web Server setting Global Catalog Port to the standard non-secure LDAP port 3268. See 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\* 7 (Intel AMT 11.8 systems only<sup>†</sup>)
- Microsoft Windows 10

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

- Microsoft Windows Server\* 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

<sup>†</sup> Windows 7 is supported on Intel AMT 11.8 systems only and will be no longer be supported after Intel AMT 16 is released.

## 1.3 Installation Prerequisites

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

- **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.

- **Operating System:** See Supported Operating Systems, section 1.2.
  - Currently, Intel EMA does not provide internationalization support. The operating system needs to have English-US Windows display language, English-US system locale, and English-US format (match Windows display language).
- **Database:** Install the Microsoft SQL Server\*. The database may run on a separate server on the network or on the same system as the Intel EMA Server. For demonstration or test purposes, Microsoft SQL Server Express edition can be used if installed with Advanced Features. For production environments, we recommend using Microsoft SQL Server Enterprise. A strong working knowledge of installing, configuring, and using SQL and Active Directory is required (if using 802.1x).



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



**Notes:**

- Microsoft SQL Server 2012, 2014, 2016, 2017, and 2019 (English-US version only) are supported.
  - The operating system of the machine on which SQL Server is running must be a supported operating system version and needs to have English-US Windows display language, English-US system locale, and English-US format (match Windows display language). See Supported Operating Systems, section 1.2.
  - Be sure to allocate enough resources (CPU, memory, SSD, etc.) to SQL Server. If your SQL Server's resources are dynamically allocated, ensure enough guaranteed fixed resources are allocated. If not, you may see error messages like "Unable to get database connection, all connections are busy" in the component server log files in **Program Files (x86)\Intel\Platform Manager\EmaLogs**.
  - Intel EMA uses query notification in SQL Server to reduce the number of database reads. That feature requires "Service Broker" to be enabled in SQL server. If Service Broker is disabled, you will see warnings to that effect in the component server log files in **Program Files (x86)\Intel\Platform Manager\EmaLogs**.
  - Before installing Intel EMA, ensure that the SQL account used in the Intel EMA SQL connection string has sysadmin rights (to create new account for IIS default application pool identity) and has at least dbcreator permission, which allows it to create, modify, and delete any database. Also, this account must have the database level roles db\_owner, db\_datawriter, and db\_datareader. The "sysadmin" right is needed in order to create new users "IIS APPPOOL\DefaultAppPool\" and "ApplicationPoolIdentity\" for the SQL server (if they do not exist). If they exist 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. See Section 1.4.18 for information about changing these permissions and roles.
- **Web Server:** Intel EMA uses Microsoft Internet Information Server (IIS). Use the latest IIS 8, IIS 8.5, or IIS 10 version.
    - Install IIS URL Rewrite Module for the target IIS. If it is installed, Intel EMA will set up the website setting to remove the IIS server version from the response header, the HSTS header, the cookie Same Site strict, and the auto redirect from HTTP to HTTPS. If it is not installed, these settings will not be applied.





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

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

- **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).
- **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.
- **Firewall:** We recommended using a firewall software to ensure that only authorized ports are available for connection. The firewall software built into Windows can perform this task.
- **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.
- **Network ports:** Table 1 lists the server network ports used for various communications among server components.
  - For certain features/usages, the AJAX server and Manageability server will establish a TCP connection (locally or remotely) with the Swarm server.
  - The endpoint and the Swarm server communicate via a secure TCP connection. Intel AMT (CIRA) and the Swarm server communicate via a secure TCP connection.
  - The Platform Manager service uses a named pipe to talk to other Intel EMA component servers on the same machine. The Platform Manager client application talks to the Platform Manager service via a secure TCP connection.

**Table 1: Server network ports**

Protocol	Port	Usage
TCP	443	HTTPS Web server port. This is used between the web browser and the web server.
TCP	1433	SQL server remote access. This is used between the internal Intel EMA server and the internal SQL server; only needed if Intel EMA server and the SQL

		server are not on the same machine. This is the default port that SQL server uses.
TCP	8000	The default TCP port for communication between Platform Manager service and Platform Manager client. You can change this port during installation.
TCP	8080	Agent, console, and Intel AMT CIRA port. This is between client endpoints and the Intel EMA Swarm server. See note below.
TCP	8084	Web redirection port. This is used between the web browser and the web server.
TCP	8089	Communication between the various Intel EMA component servers and Intel EMA Swarm server. This port number is the default, and can be changed in the Server Settings page. See "Appendix - Modifying Component Server Settings" on page 44.
TCP	8092	Port on which Ajax component server listens for internal component-to-component communication. This port number is the default, and can be changed in the Server Settings page. See "Appendix - Modifying Component Server Settings" on page 44.
TCP	8093	Port on which Swarmcomponent server listens for internal component-to-component communication. This port number is the default, and can be changed in the Server Settingspage. See "Appendix - Modifying Component Server Settings" on page 44.
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. See "Appendix - Modifying Component Server Settings" on page 44.

## 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 Back Up 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, 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 SWEET32 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 IIScripto from this website:

<https://www.nartac.com/Products/IIScripto>. This product helps to change schannels and cipher settings.

You must run the IIScripto 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).

## 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. Additionally, we recommend that you use the Diffie-Hellman Ephemeral (DHE) protocol.



**Note:** If your environment includes endpoints with Intel AMT versions below 11.8.77.3664, you need to leave TLS 1.1 enabled to ensure proper communication with these endpoints.

## 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. See section 4.2.
- 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).
  1. Skip these steps if the account already has the necessary privileges.
  2. 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. See 1.4.18 "Modify permissions of SQL Server user if desired" on page 11.
  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\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 Section 6.3, "Manageability Server" on page 46.
  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".
    - 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.
  1. Use IIS Manager to create a new app pool.
  2. Choose **.NET CLR Version v4.0.XXX**, **Integrated** pipeline mode, and **Start app pool immediately**.
3. Assign an account to the new application pool.
  1. Use IIS Manager to change the account for the new app pool.
  2. 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 verify 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, see 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.

**Table 2: Headers added to web.config**

Header	Value
X-Content-Type-Options	nosniff

X-XSS-Protection	1; mode=block
X-Frame-Options	SAMEORIGIN
Referrer-Policy	strict-origin
Expect-CT	max-age=86400, enforce
Feature-Policy	payment 'none'; microphone 'none'; geolocation 'none';
strict-transport-security	max-age=31536000; includeSubDomains;
<b>Note:</b> Added by IIS rewriter rule	
Content Security Policy (CSP)	default-src 'self' blob;;script-src 'self' 'unsafe-inline' 'nonce-<autogen_value> ' 'sha256-<multiple values> ';
<b>Note:</b> Added by plugin	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](http://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.

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. See 1.4.18 "Modify permissions of SQL Server user if desired" 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 Section 6.3, "Manageability Server" on page 46.
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".
  - 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".

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

After installation, the SQL account used by Intel EMA needs to execute stored procedures and run database commands. Therefore, this SQL account needs db\_owner, db\_datawriter, and db\_datareader permissions for the Intel EMA database. These permissions are granted by default during Intel EMA installation. If you do not want to give db\_owner permission, you must grant this SQL account 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>

## 1.5 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 communicate 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
  - See the *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
  - See the *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
  - See the *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
  - See the *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 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
  - See the *Intel® EMA Administration and Usage Guide* for 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 <ul style="list-style-type: none"> <li>• EMALog-XXX.txt</li> <li>• TraceLog-XXX.txt</li> </ul>	A log for each server component. These are the same log messages that you can see in the Platform Manager's Event log.
C:\Program Files\Intel\Ema Agent	Install location for 64 bit Intel EMA Agent files. For 32 bit agent, see Program Files (x86).
C:\inetpub\wwwroot	IIS web site locations.

## 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 table shows testing results that may be helpful in determining the appropriate server hardware configuration for your Intel EMA server installation. The table shows the number of managed endpoints required to achieve the thresholds in the column headings (e.g., 80% CPU utilization) given the server 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 envir-

onmental 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 4 CPUs and 16 GB of RAM to satisfactorily support approximately 82K managed endpoints (the 10% memory 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 4 CPUs and 16 GB of RAM in an implementation where CIRA will be used, we recommend no more than approximately 33K managed endpoints ( $82K/2 * .80 = 32.8$ ).

**Table 3: Scaling Consideration Data**

	Intel EMA 80% CPU	Intel EMA 100% CPU	Intel EMA 10% mem	DB 80% CPU	DB 100% CPU
<b>2 CPU, 8 GB mem</b>	166,389	207,969	44,600	155,775	195,145
<b>4 CPU, 16 GB mem</b>	349,636	436,972	82,180	290,036	363,566
<b>8 CPU, 32 GB mem</b>	447,525	559,256	130,977	165,275	207,029

## 2 Installing or Updating the Intel® EMA Server

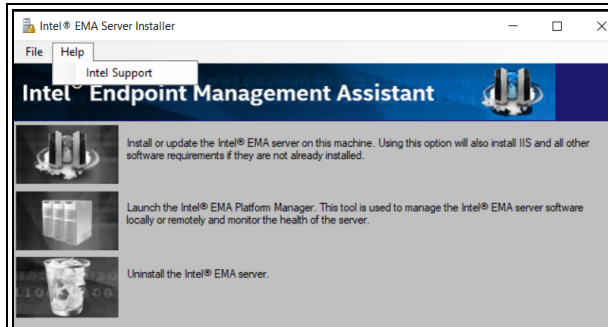
Follow the steps below to install the Intel® EMA server. For updating, see section 2.2.



### General Installation Notes:

- 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 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. See section 6 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 Section 1.4.17), 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) feature of Intel EMA allows you to mount a remote disk image (.iso or .img) to a managed endpoint via Intel AMT. To enable the USBR feature, the installer creates a 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 via USB Redirection. For more information on the USBR feature, see the section titled **USB Redirection** in the *Intel® EMA Administration and Usage Guide*.
- Version 1.5.0 of Intel EMA introduces a Web server setting for the LDAP connection port, with a default of port 636. This setting is used in 802.1x configuration. Previous Intel EMA versions would have used port 389 for LDAP. After installing v1.5.0, check your LDAP port settings in your environment to ensure you can use port 636 (or you can change the port in the Web server setting on the Server Settings page). If you experience problems with 802.1x setup during Intel AMT provisioning, this could be the issue.
- If you are installing or updating to version 1.5.0 of Intel EMA using Active Directory (AD), and you have configured AD to use non-default ports, you may experience issues installing and using Intel EMA. You can use the Intel EMA API **POST /api/latest/accessTokens/getUsingWindowsCredentials** to verify the current AD username/password with Active Directory (see the "AccessToken.htm" "Authentication" block in the sample code included with the installation package). If this API fails, either enable LDAPS secure port 3269 (recommended) or change the Web Server setting Global Catalog Port to the standard non-secure LDAP port 3268. See the following link for more information: <https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/config-firewall-for-ad->

## 2.1 Installing Using the Setup Wizard

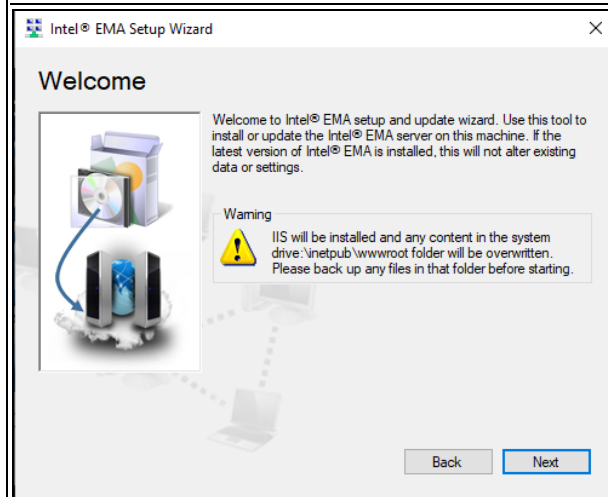


Extract the installation ZIP file, open the folder, and right-click on EMAServerInstaller.exe and select **Run as administrator**. The installer opens and the status bar at the bottom shows Ready if the initial checks have passed.

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



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

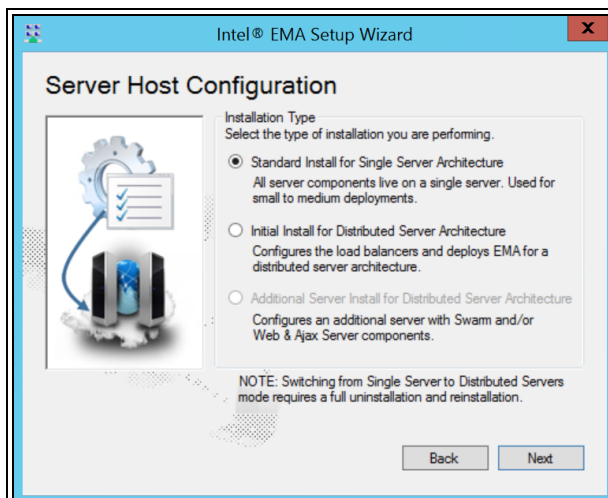


**WARNING!** For first-time installations, if you continue with the installation process, the Intel EMA Setup Wizard will delete everything in the c:\inetpub\wwwroot folder. Be sure to backup any needed files before continuing with the installation process.

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.

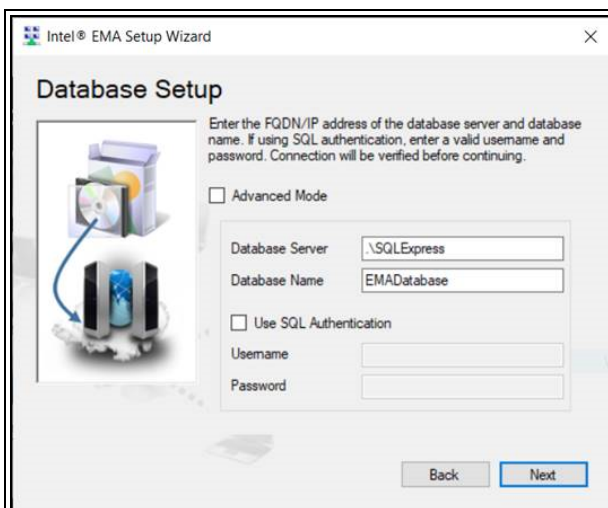
Click **Next** on the Welcome screen to continue the setup process.

### 2.1.1 Server Host Configuration



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

## 2.1.2 Database Settings

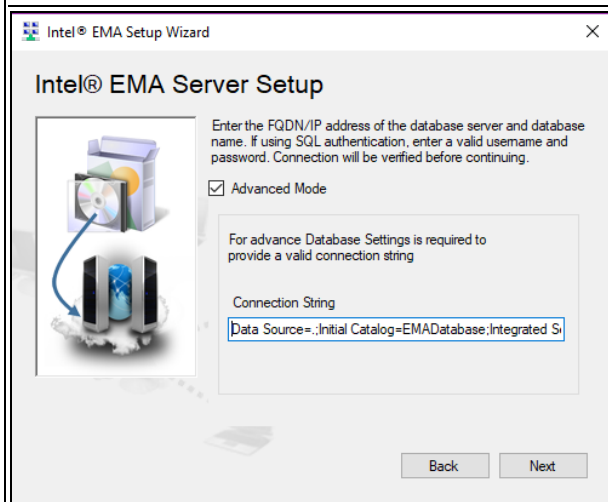


Specify the server where the database is hosted. The actual value depends on the database server you installed. Refer to your SQL installation for details.



### Notes:

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



To create a customized database connection string, click the checkbox for **Advanced Mode** and enter a connection string.

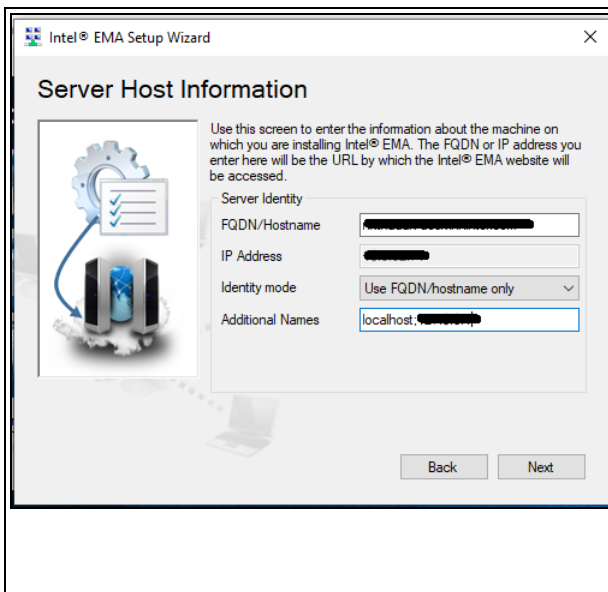
Note that both Basic and Advanced modes create a connection string which is used by the Intel EMA component servers. Advanced Mode allows you to create a customized connection string. For more information about connection strings, see <https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax>. Note that some examples on this page may not be supported by Intel EMA.



**Note:** The parameter “MultipleActiveResultSets=True” is required.

Regardless of mode (Basic or Advanced), the connection string is encrypted and stored in **c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config**.

## 2.1.3 Server Host Information



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

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

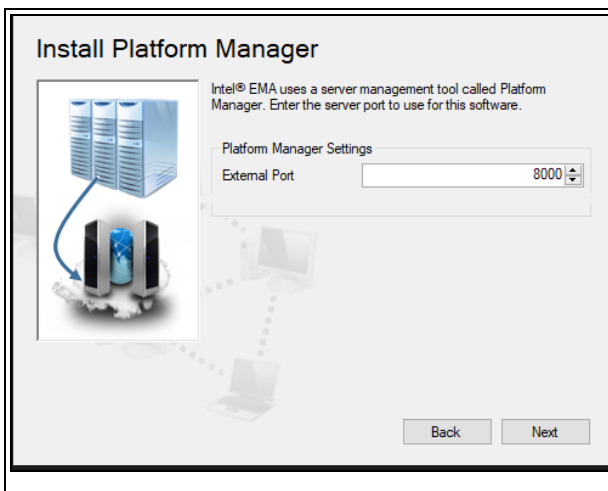
**For Identity mode:**

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



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

## 2.1.4 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.

## 2.1.5 User Authentication

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

### 2.1.5.1 Normal Accounts



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

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

### 2.1.5.2 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:** If you are installing or updating to version 1.5.0 of Intel EMA using Active Directory (AD), and you have configured AD to use non-default ports, you may experience issues installing and using Intel EMA. You can use the Intel EMA API **POST /api/latest/accessTokens/getUsingWindowsCredentials** to verify the current AD username/password with Active Directory (see the "AccessToken.htm" "Authentication" block in the sample code included with the installation package). If this API fails, either enable LDAPS secure port 3269 (recommended) or change the Web Server setting Global Catalog Port to the standard non-secure LDAP port 3268. See the following link for more information: <https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts>.



## 2.1.6 Global Administrator Account Setup



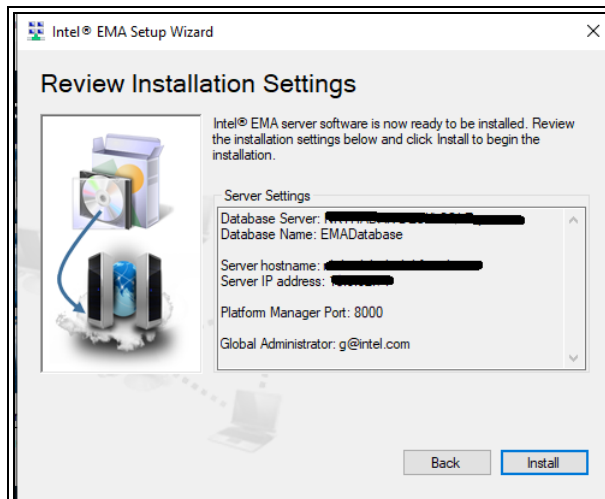
This screen only appears during setup if you have chosen “Normal accounts” for user authentication. If using domain accounts, the user running the installer will be made a Global Administrator.



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

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

## 2.1.7 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.



**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
APPP00L\DefaultAppPool] FROM WINDOWS() - System.Data.SqlClient.SqlException
(0x80131904): User does not have permission to perform this action.
```

At this point, you are ready to begin using the Intel EMA Server's Platform Manager, as described in Section 4.

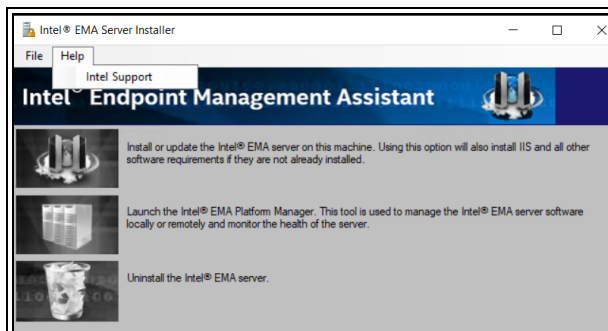
## 2.2 Performing an Update Installation Using the Setup Wizard

Follow the steps below to perform an update installation using the Intel EMA setup wizard.



### Update Installation Notes:

- 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). See section 6.1 for details.
- For updates from previous Intel EMA versions, the installer detects the connection string automatically.

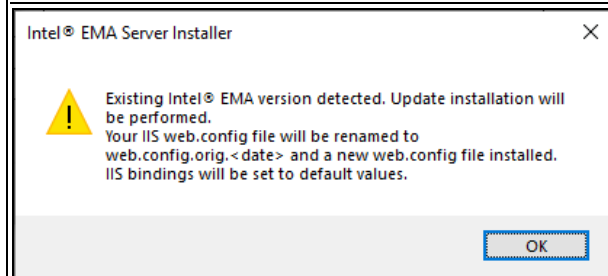


Extract the installation ZIP file, open the folder, and right-click on EMAServerInstaller.exe and select **Run as administrator**. The installer opens and the status bar at the bottom shows Ready if the initial checks have passed.

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

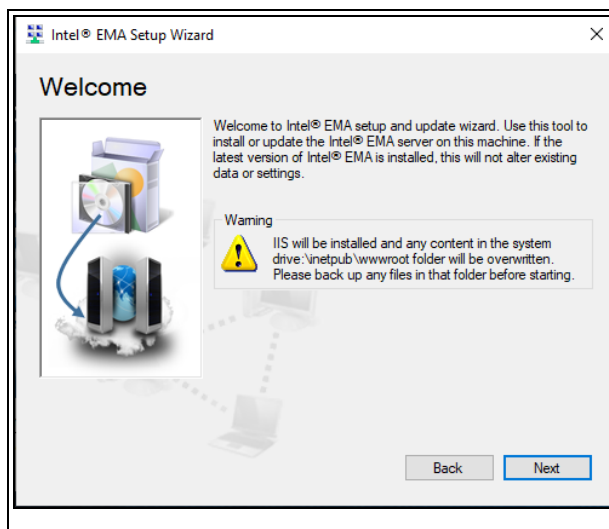


**Note:** For assistance, click **Help > Intel Support**



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**.

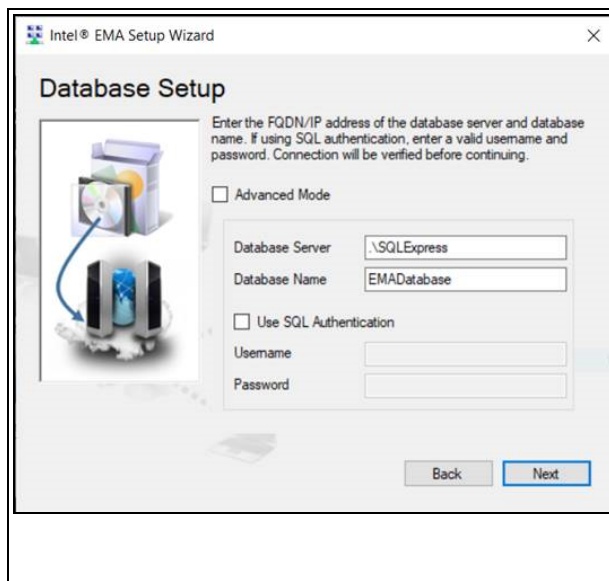


Click **Next** on the Welcome screen to continue the setup process.



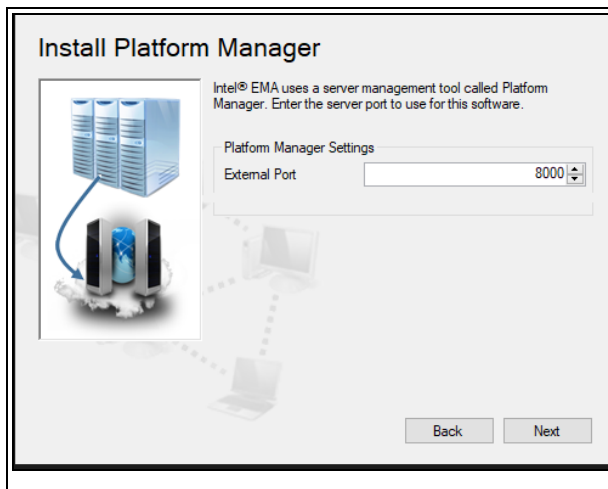
**Note:** The warning regarding IIS being installed does not apply to update installations.

## 2.2.1 Database Settings



**Note:** For update mode, the fields are filled in and cannot be changed.

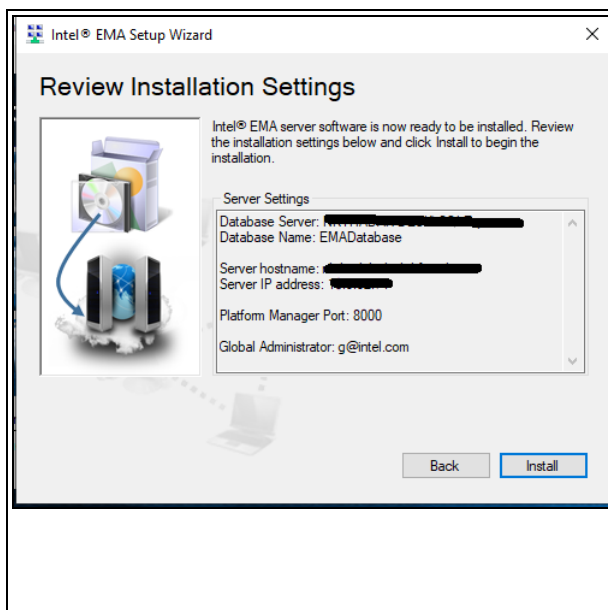
## 2.2.2 Platform Manager Configuration



**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.

## 2.2.3 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.

## 2.3 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 EMAServer-Installer.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 that 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. For more information about connection strings, see <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. Regardless of mode (Basic or Advanced), 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 (USB-R) feature, which allows 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. For more information on the USB-R feature, see the section titled **USB Redirection** in the *Intel® EMA Administration and Usage Guide*.

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

## 2.3.1 Basic Mode

Use the command syntax template below and replace the placeholder values <in brackets> to install using normal user accounts. For more options including domain authentication, run the executable with the --help option by itself.

```
EMAServerInstaller.exe FULLINSTALL --host=<server_fqdn> --dbserver=<db_server_address>
--db=<db_name> --dbuser=<SQL_user> --dbpass=<SQL_password> --guser=<global_admin_email>
--gpass=<global_admin_password> --verbose --console --accepteula
```

For the connection to the server machine, you can also use the following structure:

```
--host=<name of FQDN of the server machine > --ip=<IP of the server machine > [--ipfirst|
--hostfirst]
```

If you want Intel EMA to use the IP to connect first, use the --ipfirst flag. If you want Intel EMA to use FQDN to connect first, use the --hostfirst flag.

For the database connection, use the following:

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

SQL Authentication: --db=<DBName> and --dbserver=<DBServerName>  
--dbuser=<UserId> --dbpass=<Password>

If you want to install under “user name/password” mode (i.e., normal account mode), the command line structure requires you to enter a username and password for the global administrator. These required parameters are identified as follows:

For global administrator setup: --guser=<UserName> --gpass=<UserPassword>.

If you want to install under “domain/window authentication” mode, specify `--domainauth` flag and do not enter `--guser`, `--gpass`.

The example syntax template uses the `--console` option, so no GUI will be loaded and instead the installer will show progress on the screen and then return to the command prompt when completed.

At this point, you are ready to begin using the Intel EMA Server's Platform Manager, as described in Section 4.

## 2.3.2 Advanced Mode

The `--dbadvanced` parameter is used to provide a customized database connection string, which is encrypted and stored in `c:\Program Files (x86)\Intel\Platform Manager\Runtime\MeshSettings\connections.config`.

Use the command syntax template below and replace the placeholder values <in brackets> to install using normal user accounts. For more options including domain authentication, run the executable with the `--help` option by itself.

```
EMAServerInstaller.exe FULLINSTALL --host=<server_fqdn> --dbadvanced= "<connection_string>" --guser=<global_admin_email> --gpass=<global_admin_password> --verbose --console --accepteula
```

For more information about connection strings, see <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.

## 2.3.3 Performing an Update Installation Using the Command Line



### Update Installation Notes:

- 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). See section 6.1 for details.
- For updates from previous Intel EMA versions, the installer detects the connection string automatically.

Use the command example below to update each Intel EMA server machine in an existing distributed server architecture installation.

```
EMAServerInstaller FULLINSTALL --accepteula -c -v
```



**Note:** For updates from previous Intel® EMA versions, only the `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.

## 2.4 Uninstalling

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



#### Notes:

- 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.

## 2.4.1 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.
 

**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.
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.

## 2.4.2 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
```



**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.

## 2.5 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.

<b>File</b>	<b>Advanced Mode</b>
-------------	----------------------

	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).
<b>Database</b>	<b>Update Database</b> Launches the Update Database Settings dialog. Use this to update your database connection string post-installation.
<b>Settings</b>	<b>Sync Web Server Settings</b> Restarts the Intel EMA Web Server to apply/sync changes to web server settings.
<b>Actions</b>	<b>Setup Firewall Rules</b> Runs the portion of the installer that handles firewall rule configuration. <b>Clear Firewall Rules</b> Runs the portion of the uninstaller that resets firewall rules. <b>IIS Registration</b> Runs the Microsoft.NET aspnet_regiis.exe <b>Dump all features to file</b> Writes the enabled Windows features to a file, and writes disabled Windows features to another file. <b>Check Common Names</b> Displays the hostname, FQDN, IP addresses of this machine. <b>Check Software</b> Displays IIS version, .NET CLR version, OS version, .NET framework. <b>Domain Detection</b> Detects what domain the system running the installer is part of. <b>Uninstall the Intel EMA Server</b> Uninstalls the Intel EMA server.
<b>Manager</b>	<b>Launch Intel EMA Platform Manager</b> Launches the Intel EMA Platform Manager
<b>Help</b>	<b>Intel Support</b> Opens the Intel support portal in a web browser.



# 3 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.

At the right of the Global Administrator **Overview** page are “Quick links”, which provide shortcuts for the most common operations. There is also a “Getting Started tips” link to simple tutorials for this user role.

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” authentication mode was selected during installation.

Click the user name in the top bar 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 **Quick links** at top right. Or, from the **Users** page (available from the navigation bar at left), select the **Tenants** tab and click **New Tenant**.
2. Enter a **Tenant Name** and **Description**, then click **Save**.

The new Tenant is created, and the **Manage Tenants & Users** page is displayed.

To delete a Tenant, select the Tenants tab on the Manage Tenants & Users page, then click the ellipsis (...) 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 User Groups

To create a new User Group, do the following:

1. From the **Users** page (available from the navigation bar at left), select the **User Groups** tab and click **New Group**.
2. In the **New Group** dialog, enter a **Group name**, **Description**, and specify **Access Rights**, then click **Save**.

To delete a user group, go to the **User Groups** tab of the **Manage Tenants & Users** page, click the ellipsis (...) for the target user group and select **Delete Group...**

## 3.3.2 Adding, Modifying, and Deleting Users

To add a user, do the following:

1. From the **Overview** page, click **Add or remove users** under **Quick links** at top right. Or, from the **Users** page (available from the navigation bar at left), select the **Users** tab.
2. Select which tenant to manage users for, and click **New User**.
3. In the **New User** dialog, enter a valid email address for **User name**, then enter a **Password** (and confirm), and **Description**.
4. Select a Role for this user and click Save.

To delete a user, go to the **Users** tab of the **Manage Tenants & Users** page, click the ellipsis (...) for the target user, and select **Delete**....



### Notes:

- The last Global Administrator user cannot remove its account, nor edit it.
- If you configured Intel EMA to use Active Directory authentication, ensure the username of any user you create corresponds to the userPrincipalName attribute of the Active Directory user. The Password field is not shown or needed in this mode.

To edit a user, go to the **Users** tab of the **Manage Tenants & Users** page, click the ellipsis (...) for the target user, and select **Edit**....

If you are editing your own user account, in order to change the password, you will need to enter your current password first. If you are editing other accounts (that your role can manage), you do not need to enter the user's current password.

For “locked” users, use the **Edit** option to unlock the user's account.

# 4 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. See Section 1.4.17 for details.

## 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.

## 4.3 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

1. Start the Intel EMA Platform Manager application like any other normal Windows desktop application. Alternatively, you can run the Intel EMA installer **EMAServerInstaller.exe** (run as Administrator) and select **Manager > Launch Intel EMA Platform Manager** from the menu bar.
2. 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.
3. Enter the **Intel® EMA Web Server Identifier**. This is the hostname/FQDN/IP Address you use to open the Intel EMA website.
4. If you configured the service for Mutual TLS, select a **Client Authentication Certificate**.
5. Click **OK**.
6. If prompted, verify and **Accept** the Server Certificate.
7. In the **Connection Credentials** dialog, enter the username and password for the Global Administrator user. If you are using Windows Authentication, select **Use Windows Authentication** and then click **OK**. If you 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.

8. 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.

### 4.3.2 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.

### 4.3.3 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.
- **TerminalSessions:** Number of terminal sessions (used for the Serial-Over-LAN feature and the file browsing feature) issued by Intel EMA JavaScript library, which are process by 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.

### 4.3.4 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 log-path.

#### 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.
- **restart:** Restart the AJAX server.
- **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.
- **mcoun:** Print the count of different types of test blast messages sent via TCP connections between Intel EMA components.
- **triggertaskscheduler:** Task scheduler normally checks if there is any scheduled task to run periodically. This will trigger the checking immediately.
- **getcompletedtransactions:** Print the information for completed metadata uploads.
- **getpendingtransactions:** Print the information for pending metadata uploads.


#### 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.
- **dbcount:** Control DB trace counting.
- **dbcleanup:** Performs on-demand database maintenance routine. See Section 4.6 for details.
- **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.
- **restart:** Restart the Swarm server.
- **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 white 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.
- **bannode:** Add an endpoint to banned list.
- **clearnodeaccess:** Clear the banned and white list in memory. It will be reloaded when Swarm server starts again.
- **nodeaccesslist:** Print the endpoint white/banned list.
- **ipblocklist:** When Swarm server gets an Intel AMT CIRA or Intel EMA agent connection request, if there exists a non-empty IP block list, it will check it. If this incoming IP address is in the same subnet as specified in the IP block list, 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

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 more information about connection strings, see <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.
7. Click **Update** to update the connection string and close the Update Database Settings dialog.



**Note:** The parameter "MultipleActiveResultSets=True" is required.



**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 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. See Section 6.3 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:

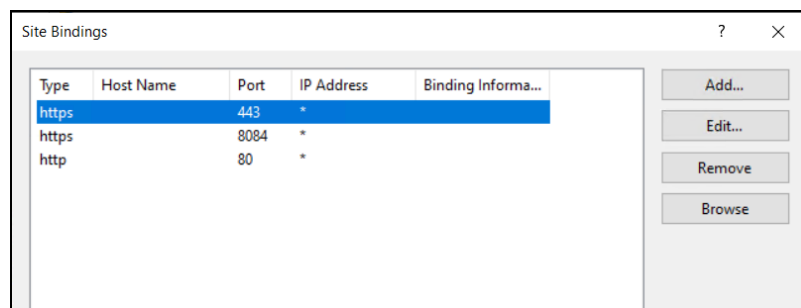
1. Run the Platform Manager (see Section 4.3.1 for details).
2. From the navigation pane at left, select **Intel® EMA Servers > localhost > EMAManeabilityServer**.
3. Select the **Console** tab.
4. In the **Component Console** window, enter the command `dbcleanup` at the prompt and press **Enter**.

## 4.7 Restoring the Intel® EMA Server from Backup

In Section 1.4.1, 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 Section "Installing or Updating the Intel® EMA Server" on page 15. 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):

?

×

Edit Site Binding

Type:

https

IP address:

All Unassigned

Port:

443

Host name:

☐ Require Server Name Indication

☐ Disable HTTP/2

☐ Disable OCSP Stapling

SSL certificate:

Select...

View...

Choose EMA's web site TLS cert

OK

Cancel

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:

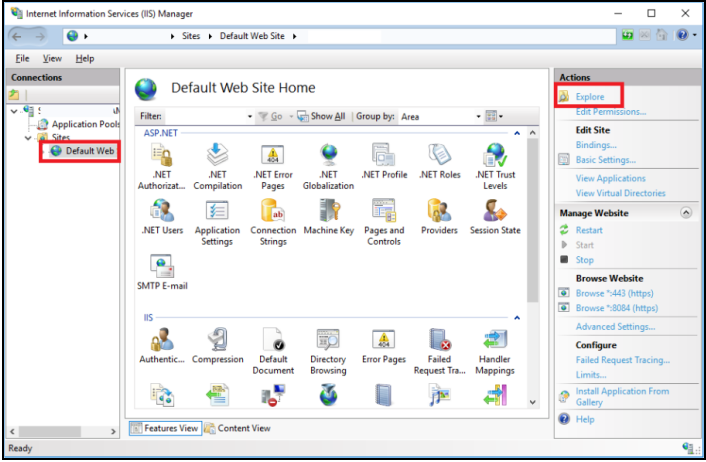
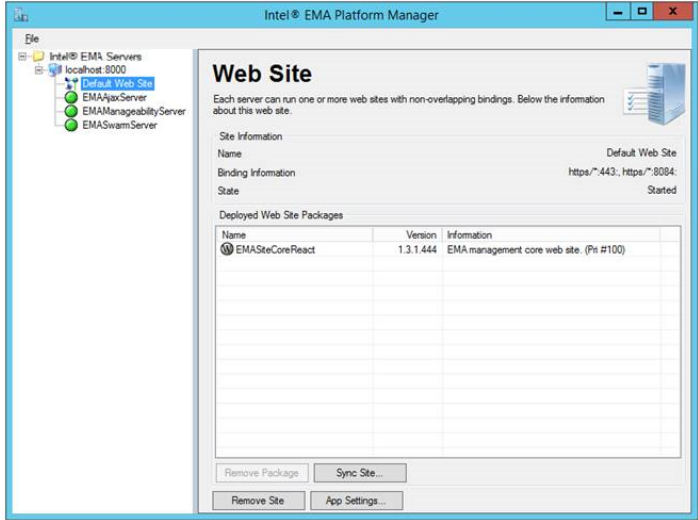
Name	Input	Match	Pattern
redirect to https	URL path after '/' {HTTPS}	Matches Matches the Pattern	* off



Outbound rules that are applied to the headers or the content of an HTTP response:

Name	Input	Match	Pattern	Action Type	Action Value	St...
Remove Server in respo...	RESPONSE_SE...	Matches	*	Rewrite	no value	F...
Add HSTS header when ...	RESPONSE_Str... (HTTPS)	Matches Matches the P...	on *	Rewrite	max-age=315...	F...
Add SameSite to cookie	RESPONSE_Set...	Matches	*	Rewrite	{R:0}; SameSit...	F...

# 5 Appendix: Troubleshooting After Installation

<p><b>Check logs, traces, or events</b></p>	<p>The installation log file <b>EMALog-Intel®EMAInstaller.txt</b> is located in the same folder as the Intel EMA installer (i.e., wherever you downloaded and ran the installer).</p> <p> <b>Note:</b> 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.</p> <p>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.</p> <p>Please see Section 4 of this guide for information on viewing the log file, trace file, or events for each of the Intel® EMA component servers.</p>
<p><b>Intel® EMA Server Installation Error</b></p>	<p><b>Intel® EMA Platform Manager Package path not set correctly</b></p> <p>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.</p> <p><b>To fix:</b></p> <ol style="list-style-type: none"> <li>1. Uninstall the Intel EMA Server, selecting all options.</li> <li>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).</li> <li>3. Re-install the Intel EMA Server.</li> </ol>
<p><b>Intel® EMA Platform Manager Service not starting</b></p>	<p>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.</p> <p>Check the status, events, and log of this service:</p> <ul style="list-style-type: none"> <li>• In the <b>Windows Services</b> viewer, check to see if it is started successfully.</li> <li>• In the <b>Windows Event Viewer</b>, go to Windows Logs \ System and look for entries with Level: Error and Source: Service Control Manager.</li> </ul>

	<ul style="list-style-type: none"> <li>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).</li> </ul> <p><b>To fix:</b></p> <p>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.</p>
<p><b>Error when trying to access the Intel® EMA website</b></p>	<p>Ensure the website is deployed. The website may not be deployed due to the package path issue mentioned above.</p> <p><b>To fix:</b></p> <p>Use Windows IIS Manager to determine the folder of the Intel® EMA website (click <b>Explore</b> under <b>Actions</b>, top right). In that folder you should see many subfolders and files.</p>  <p>If not, use the Platform Manager to "sync site" and redeploy the website.</p> 
<p><b>Using Internet Explorer on a Windows</b></p>	<p>The default security settings of Internet Explorer on Windows Server</p>

<b>Server machine</b>	<p>(e.g. Windows Server 2014) can cause many features of Intel EMA to not function correctly.</p> <p><b>To fix:</b></p> <p>We recommend using other web browsers (e.g., Chrome or Firefox) on Windows Server machines.</p>
<b>The target Intel® EMA website URL must match the Intel® EMA website's certificate</b>	<p>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.</p> <p><b>To fix:</b></p> <p>Ensure Intel EMA URL matches the <b>Issued to</b> field of the certificate.</p>
<b>Warnings and errors during Intel® AMT setup/provision</b>	<p>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.</p> <p> <b>Note:</b> 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.</p> <p><b>Transient warnings/errors that can be ignored</b></p> <p>Warning/Error type – OTP_REQUIRED:</p> <p>Message:Host Based Admin Setup (1st try): OTP_REQUIRED</p> <p>Message:Unable to go to admin mode, rolling back out of client mode.</p> <p>Warning/Error type – INTERNAL_ERROR due to Unauthorized WSMAN call:</p> <p>Message:Creating DotNetWSManClient object...</p> <p>Warning&gt;Error (2): Intel.Manageability.WSManagement.WSManException: The remote server returned an error: (401) Unauthorized.</p> <p>Message:Host Based Setup (1st try): INTERNAL_ERROR</p> <p> <b>Note:</b> The server will re-try the installation despite these errors until the third try.</p> <p><b>Valid warnings/errors that must be addressed</b></p> <p>PKI domain suffix not matching the PKI certificate:</p> <p>Warning/Error type – Message:Host Based Admin Setup (3rd try): AUTH_FAILED</p>

	<p>Warning/Error type – Message:Unable to go to admin mode, rolling back out of client mode.</p> <p>INTERNAL_ERROR due to Intel® Management and Security Application Local Manageability Service (LMS) not running correctly:</p> <p>Warning/Error type – Warning&gt;Error (2): Intel.Manageability.WSManagement.WSManException: The underlying connection was closed: The connection was closed unexpectedly.</p> <p>Warning/Error type – Message:Host Based Setup (3rd try): INTERNAL_ERROR</p> <p>WSManException due to Intel AMT FW requiring a reset:</p> <p>Warning&gt;Error (2): Intel.Manageability.WSManagement.WSManException: The underlying connection was closed: The connection was closed unexpectedly. ---&gt; System.Net.WebException: The underlying connection was closed: The connection was closed unexpectedly.</p> <p>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.</p> <p>Error due to full certificate store in Intel® AMT FW:</p> <p>Error: .[omitted]..... Certificate Store in firmware is full and no more certificates can be added.</p> <p>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.</p>
<p><b>Intel® AMT operation does not work, but all other features function correctly</b></p>	<p>This section applies to the scenario where Intel EMA server is installed under <b>Use hostname only</b> mode and the target endpoint is provisioned with Intel AMT CIRA.</p> <p>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.</p> <p><b>To fix:</b></p> <ol style="list-style-type: none"> <li>1. Unprovision the target endpoint.</li> <li>2. With a clean setup and a clean/unprovisioned endpoint, perform a CIRA provision and monitor the provision events. <ol style="list-style-type: none"> <li>a. To monitor, go to the EMAManageabilityServer's <b>Events</b> tab in Platform Manager. Make sure there are no errors (a few warnings are OK).</li> <li>b. On the target endpoint, open the <b>Intel® Management</b></li> </ol> </li> </ol>

	<p><b>and Security Status Tool</b> and go to the <b>General</b> tab. If the provision is successful, you should see two events: <b>Configured</b> and <b>Remote Control Connection is Enabled</b>.</p> <p>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.</p> <p>3. On the EMASwarmServer's <b>Component</b> tab (in Platform Manager), monitor the <b>ConIntelAmt</b> 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 <b>ConIntelAmt</b> value is still incorrect, continue with the remaining steps.</p> <p>4. At this point, Intel AMT CIRA firmware probably cannot resolve the hostname/FQDN. To verify this, use the <b>fixed IP address</b> mode to do a provision. If <b>fixed IP address</b> 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 <b>fixed IP address</b> mode:</p> <p>a. On the Server Settings page, change the <b>ciraserver_ip</b> setting of the Manageability server (see "Appendix - Modifying Component Server Settings" on page 44).</p> <p>b. Save settings and restart the Manageability server.</p> <p>5. Unprovision the target endpoint and re-perform the provision. This time, CIRA will use the IP address you specified above.</p>
<b>Uninstalling Intel® EMA server fails to drop the database</b>	<p>When uninstalling the Intel EMA server, you may see the warning/error: "Unable to drop database."</p> <p><b>To fix:</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>2. Right click the target database and choose <b>Delete</b>. Do not change any default values in the Delete option window. Delete the target database.</li> <li>3. If the database is not deleted, right-click the database server and choose <b>Restart</b>. After the database server is restarted, try to delete the target database again.</li> </ol>
<b>802.1x setup fails during Intel AMT provisioning</b>	<p>Version 1.5.0 of Intel EMA introduces a Web server setting for the LDAP connection port, with a default of port 636. This setting is used in 802.1x configuration. Previous Intel EMA versions would have used port 389 for LDAP. After installing v1.5.0, check your LDAP port settings in your environment to ensure you can use port 636 (or you</p>

	<p>can change the port in the Web server setting on the Server Settings page). If you experience problems with 802.1x setup during Intel AMT provisioning, this could be the issue.</p> <p>See section 6, "Appendix - Modifying Component Server Settings" on the next page</p>
<p><b>Active Directory user validation fails after updating to v1.5.0</b></p> <p><b>-OR-</b></p> <p><b>Active Directory option not available during installation or update to v1.5.0</b></p>	<p>If you are installing or updating to version 1.5.0 of Intel EMA using Active Directory (AD), and you have configured AD to use non-default ports, you may experience issues installing and using Intel EMA. You can use the Intel EMA API <b>POST</b> <b>/api/latest/accessTokens/getUsingWindowsCredentials</b> to verify the current AD username/password with Active Directory (see the "AccessToken.htm" "Authentication" block in the sample code included with the installation package). If this API fails, either enable LDAPS secure port 3269 (recommended) or change the Web Server setting Global Catalog Port to the standard non-secure LDAP port 3268. See the following link for more information:  <a href="https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts">https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts</a>.</p> <p>See section 6, "Appendix - Modifying Component Server Settings" on the next page</p>
<p><b>Intel EMA agents fail to connect to server after updating to v1.4.0 or later</b></p>	<p>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. See sections 1.4.6 and 1.4.7 for more information.</p>



# 6 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. See section 6.5 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
<b>UI: Admin Port</b> <b>API: adminport</b>	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.
<b>UI: Admin Port Local</b> <b>API: adminportlocal</b>	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
<b>UI: Log File Path</b> <b>API: logfilepath</b>	Path to the Intel EMA logfile.  Maximum: 248 characters Minimum: 2 characters
<b>UI: Enable Intel CIRA Power State Polling</b> <b>API: enableCIRAPowerPolling</b>	Enable periodic CIRA power state polling. Values are True/False. The default is True.
<b>UI: Maximum Number of Concurrent Database Connections</b> <b>API: maxdbconnections</b>	The maximum number of concurrent DB connections for this server.
<b>UI: Swarm Servers</b> <b>API: swarmserver</b>	List of active Swarm Servers. Includes Server ID and Server IP & Port (format IP Address: port).
<b>UI: Server IPs</b> <b>API: serverIps</b>	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


Setting	Description
	serverlps will include all IP addresses.
<b>UI: Message Port</b> <b>API: messagePort</b>	The TCP port this component server type is listening on to accept internal traffic from other Intel EMA components. Default 8093.
<b>UI: TCP Connection Retry</b> <b>API: tcpConnRetrySeconds</b>	Wait time between retries when establishing communication connections between Intel EMA server components.
<b>UI: TCP Connection Idle</b> <b>API: tcpConnIdleSeconds</b>	Interval between heartbeat messages sent between components once communications are established.
<b>UI: Agent Update Interval (Seconds)</b> <b>API: agentUpdateIntervalSeconds</b>	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.
<b>UI: Agent Auto Update</b> <b>API: enableAgentAuto Update</b>	Boolean. Enables or disables automatic agent update. Default: Enabled.


## 6.2 Ajax Server

Setting	Description
<b>UI: Ajax Cookie Auto Refresh Range</b> <b>API: ajaxCookieAutoRefreshRange</b>	Range in minutes in which the Ajax cookie life can be extended.
<b>UI: Ajax Cookie Idle Timeout</b> <b>API: ajaxCookieIdleTimeout</b>	Amount of time, in minutes, from when the cookie is added until it expires.
<b>UI: Http Header Access Control Allow Headers</b> <b>API: httpheader_Access-Control-Allow-Headers</b>	Additional headers to set in response to the Ajax request.
<b>UI: Log File Path</b> <b>API: logfilepath</b>	Path to the Intel EMA logfile. Maximum: 248 characters Minimum: 2 characters
<b>UI: User Access Failed Max Count</b> <b>API: userAccessFailedMaxCount</b>	Number of failed password attempts before user account is locked by the Web API.
<b>UI: Expire Sessions</b> <b>API: expiresessions</b>	Sets whether the Ajax server should expire the session or not (default is enabled).
<b>UI: Maximum Number of Concurrent Database Connections</b> <b>API: maxdbconnections</b>	The maximum number of concurrent DB connections for this server.
<b>UI: Server IPs</b>	List of machine IP addresses where this component server type is running. For

<b>Setting</b> <b>API: serverIps</b>	<b>Description</b> example, if the Ajax server is running on machine ip1, ip2, and ip3, then serverIps will include all IP addresses.
<b>UI: Swarm Servers</b> <b>API: swarmserver</b>	List of active Swarm Servers. Includes Server ID and Server IP & Port (format IP Address: port).
<b>UI: Message Port</b> <b>API: messagePort</b>	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

<b>Setting</b> <b>UI: CIRA Server Host</b> <b>API: ciraserver_host</b>	<b>Description</b> 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.
<b>UI: CIRA Server IP</b> <b>API: ciraserver_ip</b>	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.
<b>UI: CIRA Server Port</b> <b>API: ciraserver_port</b>	The port of the CIRA access server, which is the Swarm Server (or the Swarm Server load balancer in a distributed architecture). Used by the load balancer to direct incoming traffic (from CIRA) to the Swarm Server's 8080 port.
<b>UI: Log File Path</b> <b>API: logfilepath</b>	Path to the Intel EMA logfile.  Maximum: 248 characters  Minimum: 2 characters
<b>UI: Maximum Number of Concurrent Database Connections</b> <b>API: maxdbconnections</b>	The maximum number of concurrent database connections for this server.
<b>UI: USBR Images Root Directory</b> <b>API: usbrImagesRootDirectory</b>	The root directory on the Intel EMA server where uploaded bootable image files (.iso and .img) are stored. Default value is <b>C:\ProgramData\Intel\EMA\USBR</b> .   <b>Note:</b> 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.
<b>UI: Maximum USBR Image Storage Capacity per Tenant</b> <b>API: maxUsbrImageStorageCapacityPerTenant</b>	Disk space in GB each tenant is allowed for USBR image storage.  Default: 20 GB  Maximum: 50 GB

Setting	Description
<b>InGigabytes</b>	
<b>UI: Maximum USBR Image storage Capacity Per EMA Instance</b> <b>API: maxUsbrImageStorageCapacityPerEmalInstanceInGigabytes</b>	Total disk space in GB (for all tenants) allowed in this Intel EMA instance for USBR image storage.  Default: 50 GB Maximum: 500 GB
<b>UI: Maximum USBR Slot Count per Tenant</b> <b>API: maxUsbrSlotCountPerTenant</b>	Number of active USBR sessions allowed for each tenant.
<b>UI: Maximum USBR Idle time</b> <b>API: maxUsbrIdleTimeInMinutes</b>	Length of time in minutes a USBR session can be idle before being automatically terminated.
<b>UI: USBR Redirection Manager Loop Interval</b> <b>API: usbrRedirectionManagerLoopIntervalInSeconds</b>	Status polling interval in seconds for active USBR sessions.
<b>UI: USBR Redirection Throttling Rate</b> <b>API: usbrRedirectionThrottlingRateInMilliseconds</b>	<p>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.</p> <p> <b>Note:</b> 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.</p> <p>Default value: 0, max value 1000, min value 0.</p> <p>Suggested value = start at 10, increment by 10 to find appropriate rate for your network.</p>
<b>UI: File Upload Retention Period</b> <b>API: fileUploadRetentionPeriodInDays</b>	Number of days an incomplete resumable file upload would be kept, after which it would be automatically deleted.
<b>UI: File Upload Cleanup Interval</b> <b>API: fileUploadCleanupIntervalInHours</b>	Interval in hours that file cleanup process would run to process incomplete resumable files.
<b>UI: Swarm Servers</b> <b>API: swarmserver</b>	List of active Swarm Servers. Includes Server ID and Server IP & Port (format IP Address: port).
<b>UI: Server IPs</b>	List of machine IP addresses where this component server type is


<b>Setting</b> <b>API: serverIps</b>	<b>Description</b> running. For example, if the Manageability server is running on machine ip1, ip2, and ip3, then serverIps will include all IP addresses
<b>UI: Message Port</b> <b>API: messagePort</b>	The TCP port this component server type is listening on to accept internal traffic from other Intel EMA components. Default 8094.
<b>UI: Audit Log Cleanup Interval (Hours)</b> <b>API: AuditLogCleanupIntervalInHours</b>	Interval in hours before cleanup of audit log records in the Intel EMA database.
<b>UI: Audit Log Retention Period (Days)</b> <b>API: AuditLogRetentionPeriodInDays</b>	Interval in days before cleanup of audit log records in the Intel EMA database.
<b>UI: Enable 8021X Certificate Auto Renewal</b> <b>API: Is8021XCertificateRenewalEnabled</b>	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.
<b>UI: 802.1X Certificate Renewal Window (Days)</b> <b>API: Ieee8021xCertificateRenewalWindowDays</b>	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

## 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.

<b>Setting</b> <b>UI: Access Token Time to Live</b> <b>API: AccessTokenTimeToLive</b>	<b>Description</b> Expiration duration of the API bearer token, in seconds.
<b>UI: Ajax Server Host</b> <b>API: AjaxServerHost</b>	Hostname or IP address of the Ajax server, or the load balancer of the Ajax servers.
<b>UI: Enable Allowed Domains, Allowed Domains</b> <b>API: EnableAllowedDomains, AllowedDomains</b>	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).
<b>UI: Log File Path</b> <b>API: logfilepath</b>	Path to the Intel EMA logfile.  Maximum: 248 characters  Minimum: 2 characters
<b>UI: Maximum Number of Concurrent Database Connections</b>	The maximum number of concurrent database connections for this server.

Setting	Description
API: maxdbconnections	
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 Port API: SwarmServerPort	8080 in single server installation or the Swarm server port exposed by the swarm server load balancer in distributed server architecture.
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.
UI: LDAP Connection Port API: LdapConnectionPort	<p>The port used for LDAP connection in 802.1x configuration. Default port is secure 636.</p> <p> <b>Note:</b> Version 1.5.0 of Intel EMA introduces a Web server setting for the LDAP connection port, with a default of port 636. This setting is used in 802.1x configuration. Previous Intel EMA versions would have used port 389 for LDAP. After installing v1.5.0, check your LDAP port settings in your environment to ensure you can use port 636 (or you can change the port in the Web server setting on the Server Settings page). If you experience problems with 802.1x setup during Intel AMT provisioning, this could be the issue.</p>
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.

## 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.

Setting	Description
UI: Unauthorized TCP connection timeout API: enableUnauthTcpConnectionIdle Timeout	<p>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.</p> <p>Default: true.</p>

<b>Setting</b> <b>UI: TCP connection timeout</b> <b>API: unauthTcpConnectionIdleTimeoutInMilliseconds</b>	<b>Description</b> 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: 5000  Maximum: 3,600,000 (1 hour)
<b>UI: Rate Limiter</b> <b>API: enableRateLimiter</b>	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.
<b>UI: Rate Limiter Window Size</b> <b>API: rateLimiterWinSizeInMilliseconds</b>	The window size in milliseconds to use for tracking requests with per-IP address rate limiting.  Default: 200  Maximum: 3,600,000 (1 hour)
<b>UI: Ajax HTTP Requests Max Count</b> <b>API: ajaxHttpRequestRateLimiterMaxCount</b>	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
<b>UI: Message Ports Requests Max Count (Before Authorization)</b> <b>API: blastMessageBeforeAuthRateLimiterMaxCount</b>	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
<b>UI: Message Ports Requests Max Count (After Authorization)</b> <b>API: blastMessageAfterAuthRateLimiterMaxCount</b>	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
<b>UI: Swarm Admin Ports Request Max Count (Before Authorization)</b> <b>API: adminPortBeforeAuthRateLimiterMaxCount</b>	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
<b>UI: Swarm Admin Ports Request Max Count (After Authorization)</b> <b>API: adminPortAfterAuthRateLimiterMaxCount</b>	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

<b>Setting</b>	<b>Description</b>
	Maximum: 1,000,000
<b>UI: Agent Port Request Max Count (Before Authorization)</b> <b>API: agentPortBeforeAuthRateLimiterMaxCount</b>	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).  Default: 20  Maximum: 1,000,000
<b>UI: Agent Port Request Max Count (After Authorization)</b> <b>API: agentPortAfterAuthRateLimiterMaxCount</b>	The maximum number of allowed authenticated requests per-IP in a window before requests would be throttled to the Swarm Server Agent port (8080).  Default: 1000  Maximum: 1,000,000
<b>UI: Connection Count Check</b> <b>API: enableConnectionCountChecker</b>	Boolean. When enabled Intel EMA will limit the TCP TLS connection count per-IP address to help prevent Denial of Service attacks.  Default: true.
<b>UI: Message Port (connections per port)</b> <b>API: blastMessageConnCountChecker</b>	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
<b>UI: Admin Port (connections per port)</b> <b>API: swarmAdminPortConnCountChecker</b>	The maximum number of connections per-IP address allowed to the Swarm Server Admin port (8089).  Default: 20,000  Maximum: 1,000,000
<b>UI: Swarm Agent Port (connections per port)</b> <b>API: swarmAgentPortConnCountChecker</b>	The maximum number of connections per-IP address allowed to the Swarm Server Agent port (8080).  Default: 20,000  Maximum: 1,000,000



# 7 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

Please double check that these properties are set correctly.

## 7.3 Internet Explorer Used by the End User

For the domain/Windows authentication to work correctly, the Intel EMA website should be recognized as being in the **Local Intranet** zone. You can verify the zone by right-clicking on the Intel EMA web page, and then choosing Properties.

Some users may have **Display intranet sites in Compatibility View** selected (checked) under the **Compatibility View Settings** in Internet Explorer. This needs to be unchecked; otherwise, the Intel EMA website will not work correctly.

## 7.4 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.

## 7.5 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.

## 7.6 References

- <https://blogs.msdn.microsoft.com/chiranth/2014/04/17/setting-up-kerberos-authentication-for-a-website-in-iis/>
- <https://blogs.msdn.microsoft.com/webtopics/2009/01/19/service-principal-name-spn-checklist-for-kerberos-authentication-with-iis-7-07-5/>
- <https://support.microsoft.com/en-us/help/326214/how-to-configure-user-and-group-access-on-an-intranet-in-windows-serve>
- <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\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831722(v=ws.11))

# 8 Appendix – Configuring Network Infrastructure for 802.1X Authentication

This section is intended for those Intel® EMA Global Administrators who want to enable 802.1X authentication for Intel® AMT. If this does not apply to you, skip this section.

Intel EMA supports Extensible Authentication Protocol (EAP), which is compatible with Microsoft's implementation of the RADIUS specification, the Network Policy Server (NPS).



**Note:** This section focuses on configuration for the Intel EMA server system to enable 802.1x usage overall. For information on configuring an 802.1x profile for a specific Tenant usage space, see the *Intel® EMA Administration and Usage Guide*.

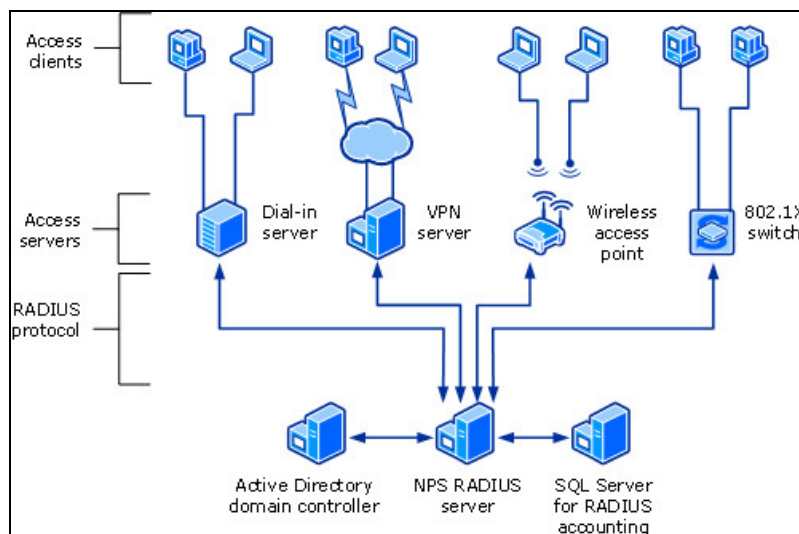
## 8.1 RADIUS Server - NPS

NPS is Microsoft's implementation of the RADIUS standard specified by the Internet Engineering Task Force (IETF) in RFCs 2865 and 2866. As a RADIUS server, NPS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless, authenticating switch, dial-up and virtual private network (VPN) remote access, and router-to-router connections.

NPS enables the use of a heterogeneous set of wireless, switch, remote access, or VPN equipment. You can use NPS with the Remote Access service, which is available in Windows Server 2016.

The following figure shows NPS as a RADIUS server for a variety of access clients.

**Figure 1: NPS components**



To configure NPS as a RADIUS server, you can use either standard configuration or advanced configuration in the NPS console or in Server Manager. To configure NPS as a RADIUS proxy, you must use advanced configuration.

## 8.2 Configure a Microsoft NPS

### 8.2.1 Dependencies

**User database:** A database and all of the required objects for searching and authenticating users during connection attempts is required. The most common source for this is Active Directory. This guide describes the use of Active Directory as a source for configuring user authentication on the NPS.

**PKI Infrastructure:** If the 802.1X EAP protocol used requires the use of certificates, the required infrastructure and Certification Authorities must already be deployed in the domain in order for the NPS to correctly validate the credentials presented by RADIUS supplicants (endpoints).

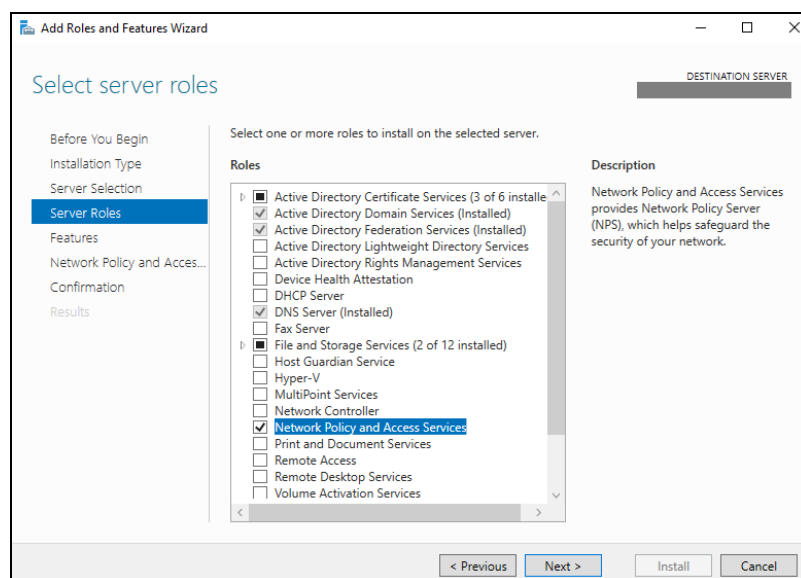
**RADIUS Clients:** Any device capable of receiving and forwarding requests and responses to and from the RADIUS server can function as a RADIUS client in this configuration. This is also true for any device capable of using the information resulting from the process to allow or deny connection to the network. For wired connections, this device is usually a Network Switch compatible with 802.1X authentication. For wireless connections, this is usually a Network Router device compatible with 802.1X authentication (WPA Enterprise or similar).

All of the dependencies listed above must be configured independently of this feature in order for the NPS deployment to proceed successfully.

### 8.2.2 Step 1 – Adding the NPS Role to Windows Server

1. From the Server Manager Console, launch the **Add Roles and Features** wizard
2. Click **Next**, and select **Role-based or Feature-based installation**.
3. Click **Next** again.
4. Select a server and click **Next**.
5. In the Server Roles panel, select **Network and Policy Access Services** and click **Next**.

**Figure 2: Select server roles**

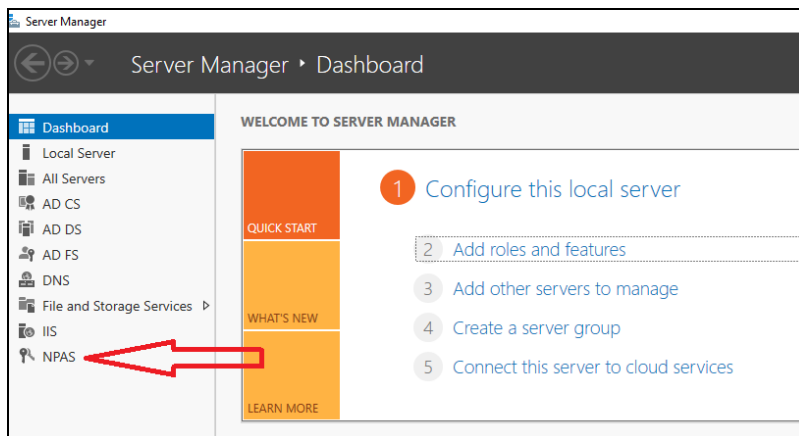


(If requested, check the **Install Management Tools** box.)

6. Click **Next** on the Features panel.
7. Click **Next** on the Network and Policy Access Services panel.

8. On the Confirmation panel, verify the configuration and click **Install**. If asked to reboot, proceed.
9. When the configuration is complete, click Finish and close the wizard.
10. If the previous step was successful, the Network Policy and Access Services (NPAS) role should appear in the Server Manager.

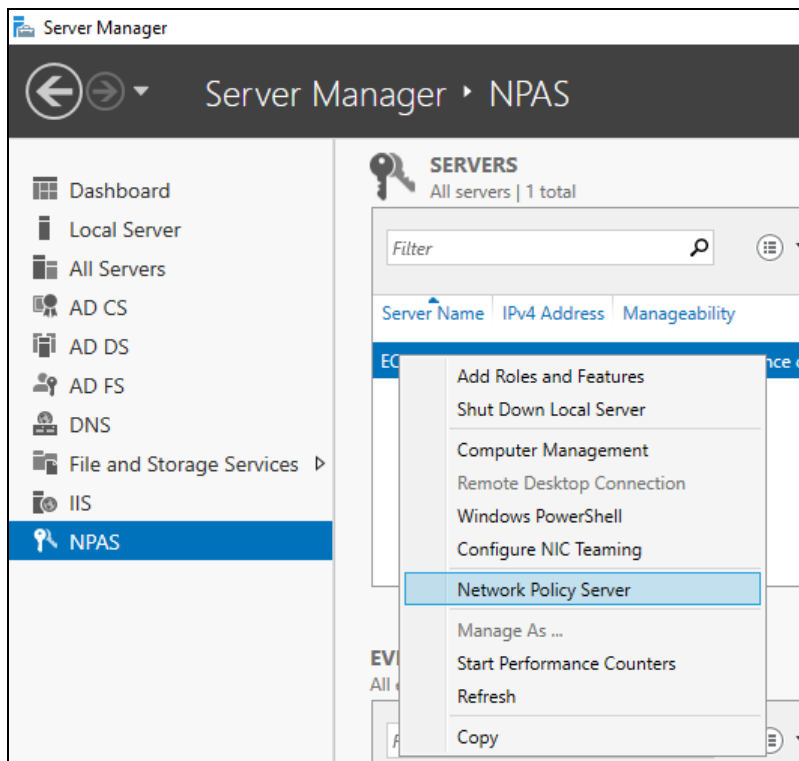
**Figure 3: NPAS role shown on the left panel**



### 8.2.3 Step 2 – Configuring NPS as a RADIUS Server

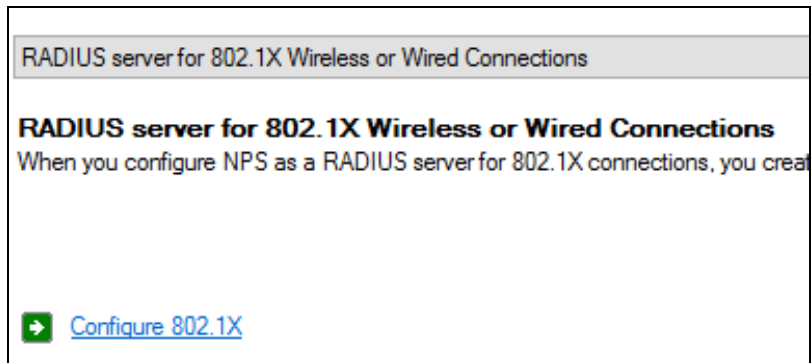
1. From the Server Manager console, select **Network Policy and Access Server**, then right-click the server and select **Network Policy Server**.

**Figure 4: Open NPS settings**



2. From the NPS Console, in the Standard Authentication section, click the **Configuration Scenario** dropdown list and select **RADIUS Server for 802.1X Wireless or Wired Connections**.
3. The configuration link below should now display "Configure 802.1X". Click the link to continue the process.

**Figure 5: Updated configuration link**



4. The **Select 802.1X Connections Type** panel lets you select the type of network (wired / wireless) connections that will be authenticated using this policy. Select Wired or Wireless connections, give the policy a name, and click **Next**.
5. The **Specify 802.1X Switches** panel lets you configure one or more RADIUS clients. These devices will route requests and responses to and from the NPS. Click **Add**, and in the resulting "New Radius Client", fill out all of the applicable information and click **OK**. Then, click **Next**.



**Important:** The shared secret must be the same on both the NPS and RADIUS clients.

6. On the **Configure an Authentication Method** panel, select the protocol and credential type to use on the policy. The example in this guide shows the configuration of the EAP-TLS protocol with certificate-based credentials.
7. Click the **Configure** button, then select the TLS Certificate presented by the NPS to the supplicants (end-points) when a connection attempt is received.



**Important:** The certificate must be issued by a Certification Authority trusted by the endpoint device.

8. Once finished, click **OK**, and then **Next**.
9. On the **Specify User Groups** panel, select all of the groups that the NPS will use to validate the client credentials when a connection attempt is received. Intel EMA supports specifying a list of Security Groups where Intel AMT devices can be added in order to facilitate 802.1X authentication. Those groups should be included in the Network Policy. Click **Next** to continue the configuration.
10. If needed, configure any applicable Traffic Control Attributes, then click **Next**.
11. Verify the configuration and click **Finish**.

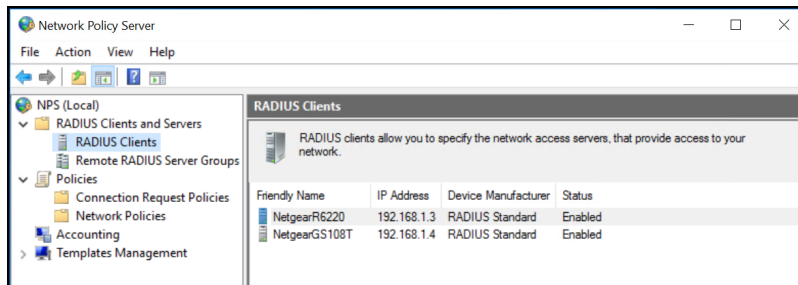
## 8.2.4 Post-configuration Actions

Perform the following actions to NPS to adjust the RADIUS server as required.

### 8.2.4.1 Create or edit a RADIUS client

1. From the left-side navigation tree in the Network Policy Server window, open **RADIUS Clients and Servers > RADIUS Client**.

Figure 6: Access the RADIUS client option



2. To create a new client, click on the section name and then click **New**. To edit an existing client, double-click on it.
3. Set the required information, especially the following:
  - **Address (IP or DNS):** This is the address of the Client device that will contact the server.
  - **Shared secret:** Create a passphrase that will be used by the actual RADIUS Client for authentication.

#### 8.2.4.2 Create or edit a Connection Request Policy

These policies will filter the requests made by the client. They will grant or reject the connections according to either the client's properties, type of network interface used, etc., and, optionally, will apply extra settings to the incoming request.

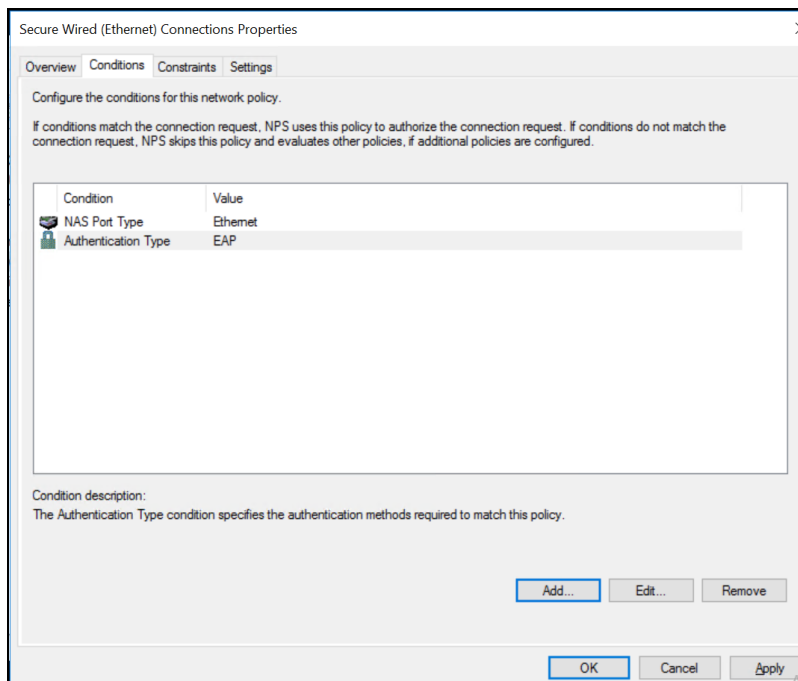
1. From the left-side navigation tree in the Network Policy Server window, open **Policies > Connection Request Policies**.
2. To create a new policy, click on the section name and then click **New**. To edit an existing policy, double-click on it.
3. Set the required configuration. In particular, set the Conditions the request should fulfill.

#### 8.2.4.3 Create or edit a Network Policy

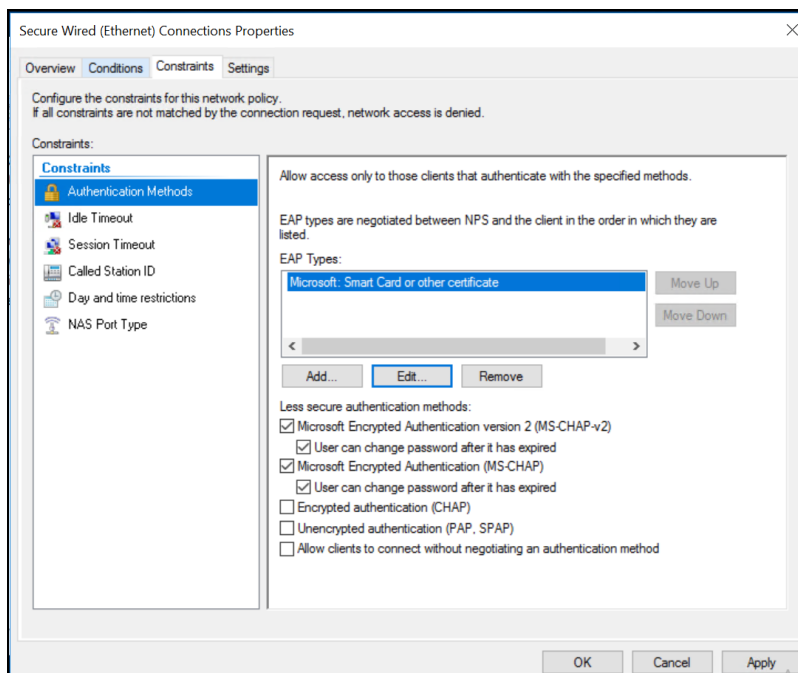
These policies will be applied to the connection in order to grant or deny access to the network. The protocol to be used by the 802.1X authentication is validated with these policies.

1. From the left-side navigation tree in the Network Policy Server window, open **Policies > Network Policies**.
2. To create a new policy, click on the section name and then click **New**. To edit an existing policy, double-click on it.
3. Set the required configuration. In particular, set the Conditions and Constraints the request should fulfill.

**Figure 7: Access the Network Policy properties (a)**



**Figure 8: Access the Network Policy properties (b)**



## 8.3 Configuring the RADIUS Clients

To configure the RADIUS clients, refer to the device's manual and follow the instructions to configure the desired network using the settings specified above.

For Wireless Access Points, the settings will usually require the following:



- Select the network to authenticate using 802.1X
- From the authentication protocol select WPA/WPA2 Enterprise
- On the RADIUS Server field, enter the IP Address or hostname of the RADIUS Server (NPS)
- On the Shared Secret, enter the same secret used to configure the RADIUS server

For Wired Ethernet switches, the settings will usually require the following:

- On the RADIUS Server configuration, enter the IP Address or hostname of the RADIUS Server (NPS)
- On the Shared Secret, enter the same secret used to configure the RADIUS server
- Enable the 802.1X configuration for Port Based Authentication
- Configure Port authentication to indicate which ports will authenticate using 802.1X

## 8.4 Connecting Endpoints to the Network

In order for devices to access the network, ensure the following:

- **RADIUS Server** – NPS properly configured, enabled and with active network policies and Connection Request policies that match the desired medium, RADIUS clients and credential types.
- **RADIUS Client** – All of the applicable network devices and Access Points are configured to forward requests and responses to and from the NPS as above.
- **Supplicant** – The endpoint device must be configured to connect to the specified network using the correct credential type. For in-band (OS) connections, this will require installing the applicable certificate on the Certificate store on the device. For out-of-band connections (Intel AMT), this will require provisioning the device using an Intel AMT Profile that fits the 802.1X settings used to configure the network.

## 8.5 Environment Setup Example

This section provides a complete configuration of an environment that implements the 802.1X authentication provisioning Intel AMT devices through Intel EMA.

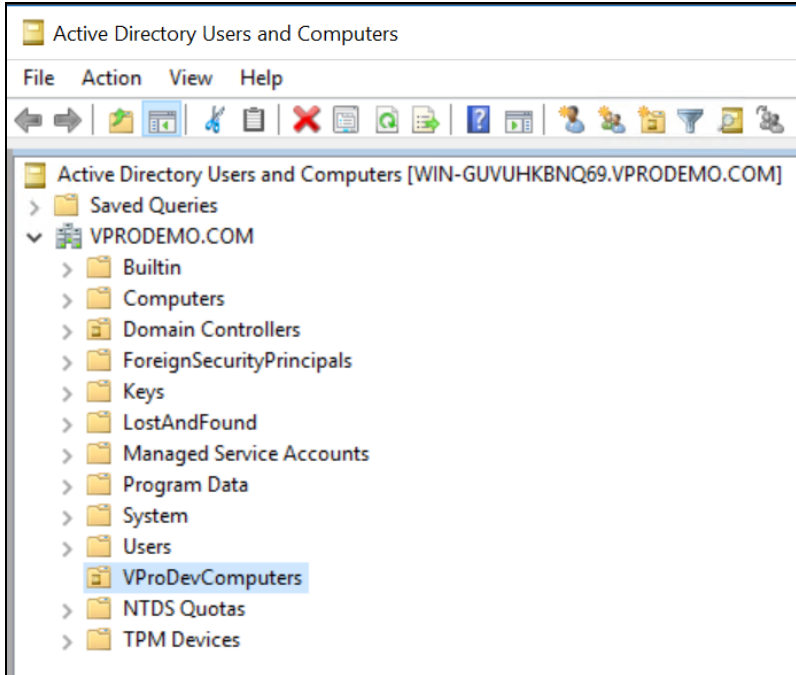
The environment is composed of the following elements:

- Windows Server 2016 Standard with the following servers, services and programs:
  - Active Directory Domain Services
  - Active Directory Certificate Services
  - DHCP Server
  - DNS Server
  - Internet Information Services
  - Network Policy Server
  - SQL Server 2016
  - Endpoint Management Assistant v1.3.2
  - Static IP Address: 192.168.1.2
- Netgear Prosafe GS108T Smart Switch for Ethernet connections
- Netgear AC1200 Smart WiFi Router Model: R6220 for Wireless connections
- Dell Latitude E7270 Intel vPro® capable Intel AMT v11.8.50 as endpoint

## 8.5.1 Active Directory Domain Services

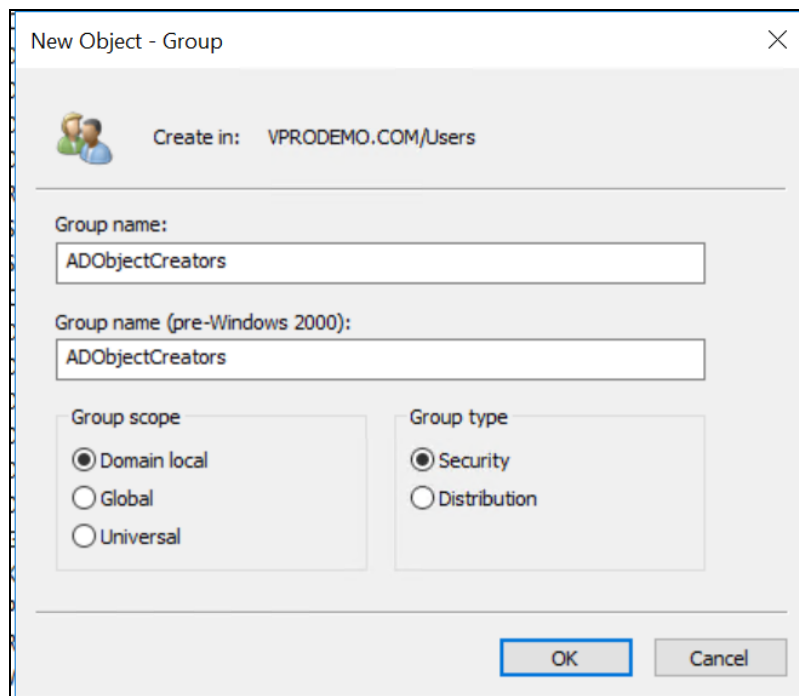
1. Add an Organization Unit under Domain: **VPRODEMO.COM**. This Organizational Unit, **VProDevComputers**, stores the Computer objects used for 802.1X authentication.

**Figure 9: Add a new Organization Unit**



2. Add privileges to the machine where Intel EMA server is running.
  - a. Create a Security Group with Group scope = Domain Local.

**Figure 10: Create a security group**



- b. Add the target Computer object to the new security group. Do this for the machine hosting the manageability server.

**Figure 11: Add computer to the new security group**

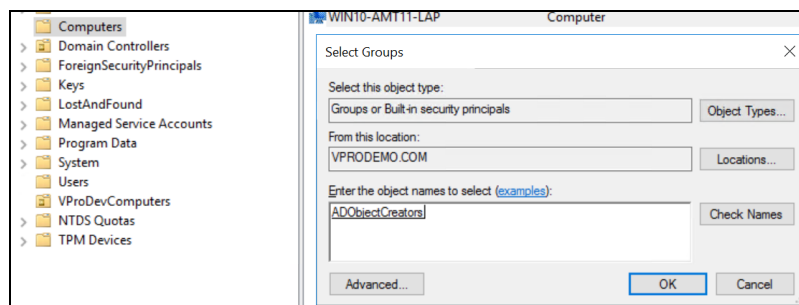
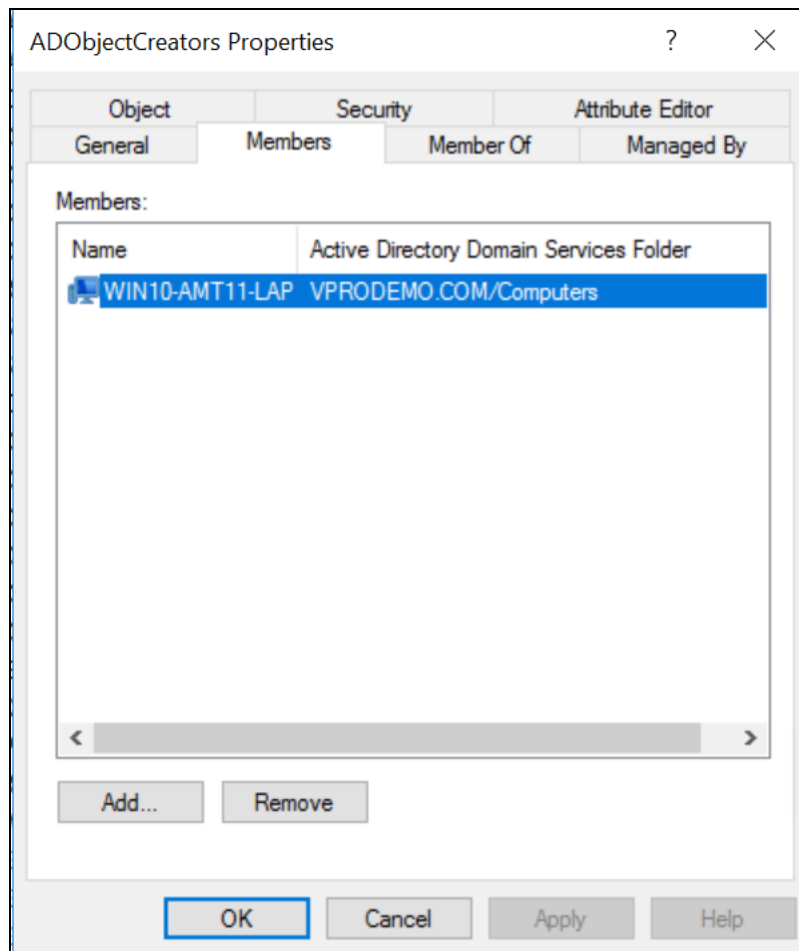


Figure 12: Modify the security group's members



- c. Add the new security group to the Security tab of the Organizational Unit where the AD Computer objects for 802.1X authentication will be created. Ensure that this 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 13: Modify Security list of the OU

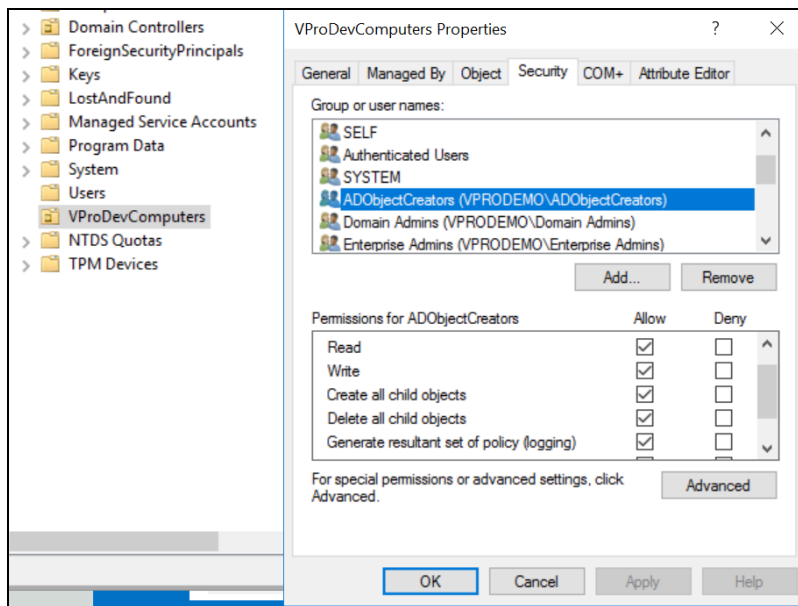
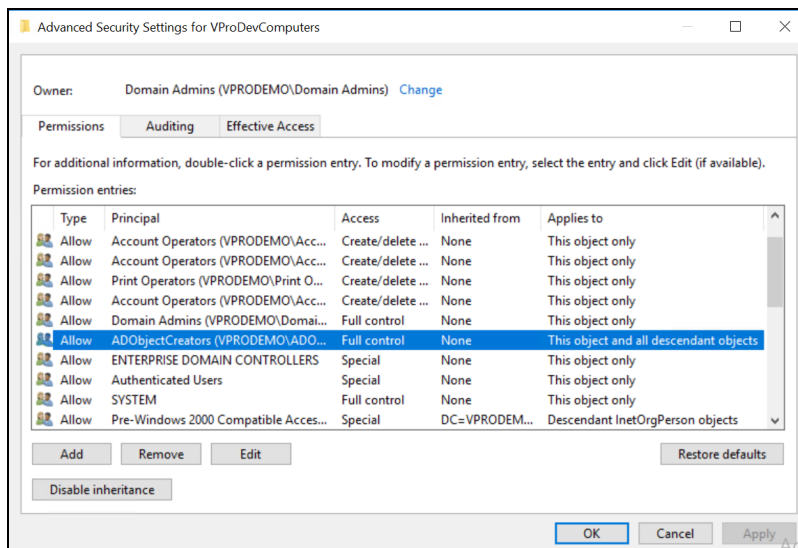


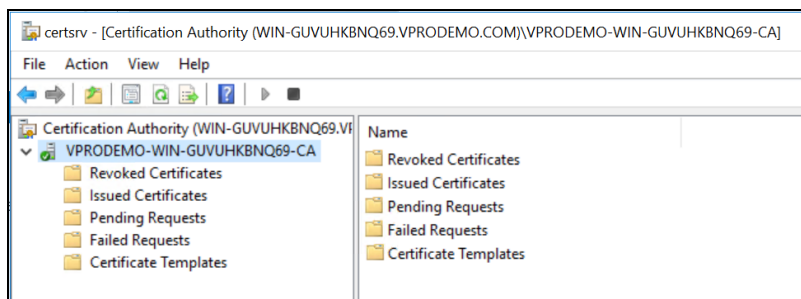
Figure 14: Modify advanced security settings



## 8.5.2 Active Directory Certificate Services

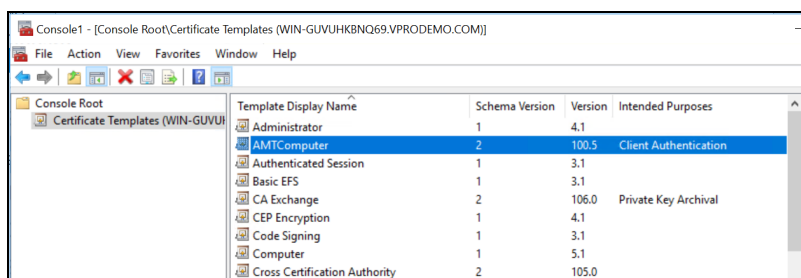
1. Choose the Certification Authority (Enterprise root CA): VPRODEMO-WIN-GUVUHKBNQ69-CA.

Figure 15: Certification Authority list



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

Figure 16: 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, select **Allow private key to be exported**.
- d. On the Security tab, grant **Read** and **Enroll** permission to **Domain Computers**. (Also add **Everyone** for manual enrollment.)
- e. Enable the template in the Certification Authority (right-click on **Certificate Template** and select **New > Certificate Template to Issue**).

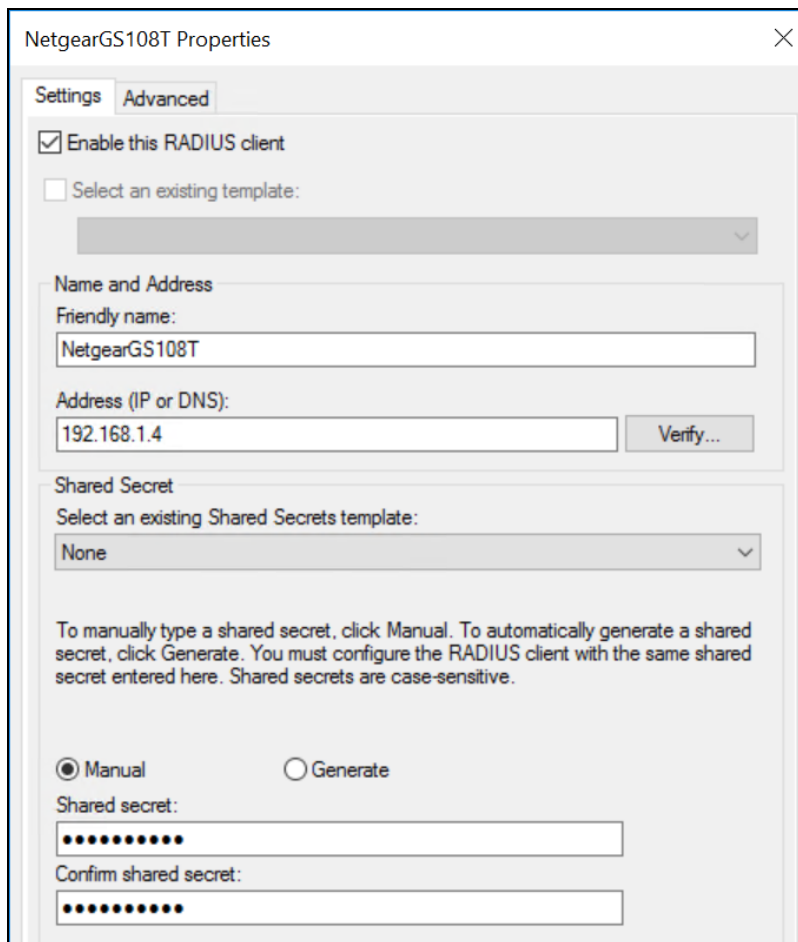
## 8.5.3 Network Policy Server

1. Set up two RADIUS clients, one for each network access point, as shown below.

Table 4: Network Policy Server RADIUS clients

Friendly Name	IP Address	Device Manufacturer	Status
NetgearGS108T	192.168.1.4	RADIUS Standard	Enabled
NetgearR6220	192.168.1.3	RADIUS Standard	Enabled

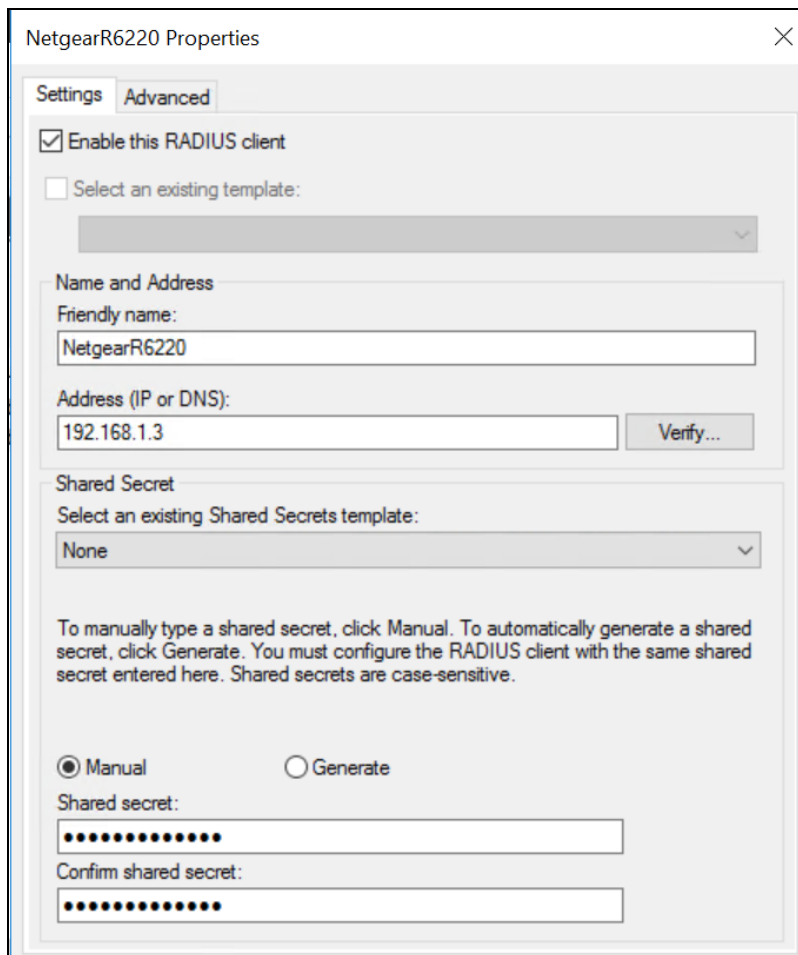
Figure 17: RADIUS client 1



The image shows a Windows-style dialog box titled "NetgearGS108T Properties" with a close button (X) in the top right corner. The dialog has two tabs: "Settings" and "Advanced", with "Advanced" currently selected. The "Advanced" tab contains the following elements:

- A checked checkbox labeled "Enable this RADIUS client".
- An unchecked checkbox labeled "Select an existing template:" followed by a dropdown menu showing a grey bar and a downward arrow.
- A section titled "Name and Address" containing:
  - A label "Friendly name:" followed by a text box containing "NetgearGS108T".
  - A label "Address (IP or DNS):" followed by a text box containing "192.168.1.4" and a "Verify..." button.
- A section titled "Shared Secret" containing:
  - A label "Select an existing Shared Secrets template:" followed by a dropdown menu showing "None" and a downward arrow.
  - A paragraph of text: "To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive."
  - Two radio buttons: "Manual" (which is selected) and "Generate".
  - A label "Shared secret:" followed by a text box filled with 12 dots.
  - A label "Confirm shared secret:" followed by a text box filled with 12 dots.

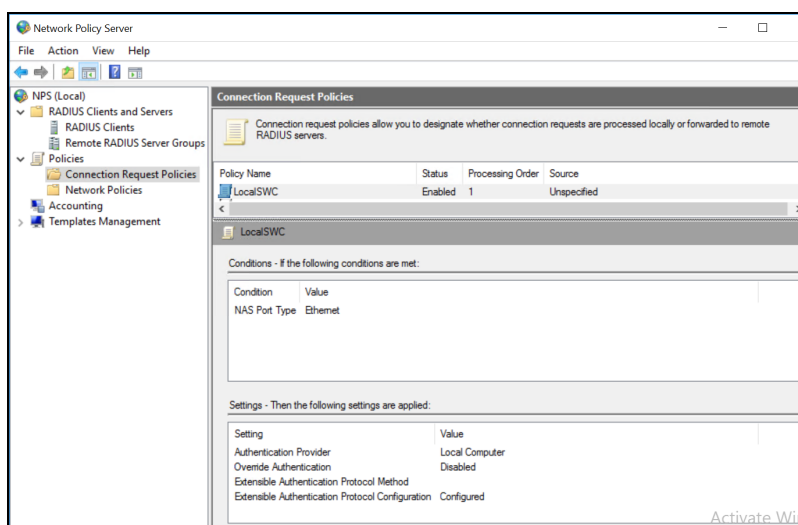
Figure 18: RADIUS client 2



The image shows the 'NetgearR6220 Properties' dialog box with the 'Advanced' tab selected. The 'Enable this RADIUS client' checkbox is checked. Below it is a dropdown for 'Select an existing template:' which is currently empty. The 'Name and Address' section contains a 'Friendly name:' field with 'NetgearR6220' and an 'Address (IP or DNS):' field with '192.168.1.3' and a 'Verify...' button. The 'Shared Secret' section has a dropdown for 'Select an existing Shared Secrets template:' set to 'None'. Below this is a text box explaining that users can manually type or generate a shared secret, noting that secrets are case-sensitive. At the bottom, the 'Manual' radio button is selected, and there are fields for 'Shared secret:' and 'Confirm shared secret:', both masked with dots.

2. Set up a Connection Request Policy.

Figure 19: NPS Connection Request Policies view

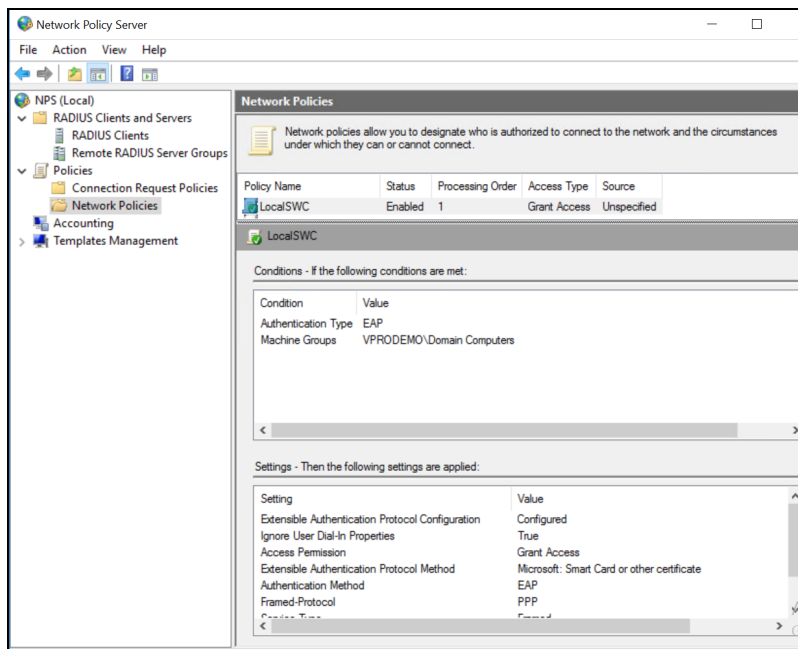


The image shows the 'Network Policy Server' console window. The left pane shows the tree view with 'NPS (Local)' expanded, and 'Connection Request Policies' selected. The right pane displays the 'Connection Request Policies' configuration for the 'LocalSWC' policy. It shows a table with columns for Policy Name, Status, Processing Order, and Source. Below this, the 'Conditions' section shows a table with 'Condition' and 'Value' for 'NAS Port Type' set to 'Ethernet'. The 'Settings' section shows a table with 'Setting' and 'Value' for 'Authentication Provider' (Local Computer), 'Override Authentication' (Disabled), 'Extensible Authentication Protocol Method' (Configured), and 'Extensible Authentication Protocol Configuration' (Configured). An 'Activate Windows' watermark is visible in the bottom right corner.

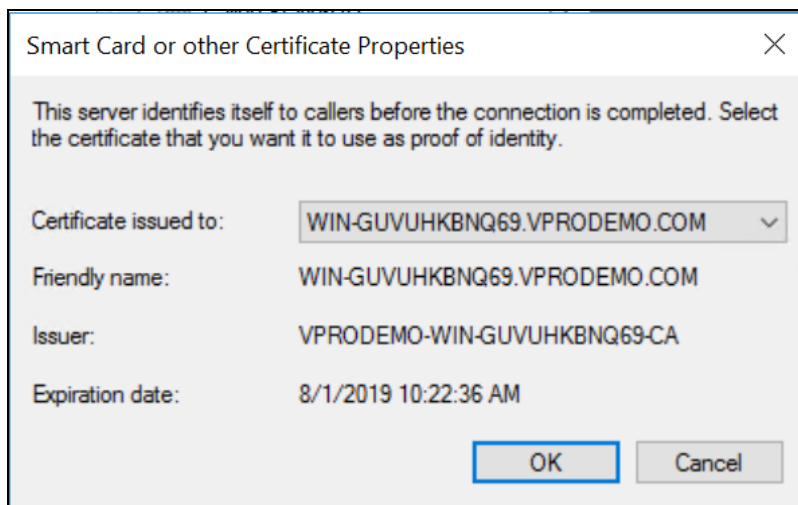


3. Set up a Network Policy, used to evaluate connections using EAP-TLS protocol, indicating the following properties:
  - Conditions: Authentication Type = EAP
  - Constraints: Authentication Methods. EAP Types: Microsoft: Smart Card or other certificate

**Figure 20: NPS Network Policies view**



**Figure 21: EAP Types: Microsoft: Smart Card or other certificate properties**

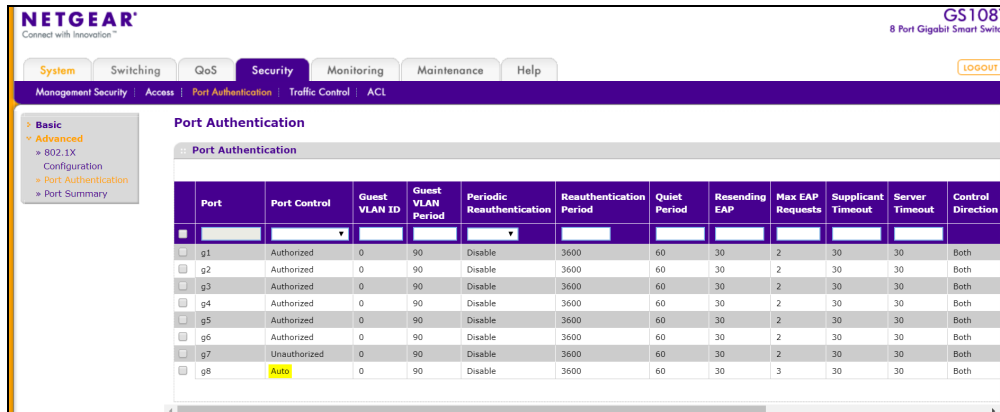


## 8.5.4 Wired Connection

The example below uses an Ethernet switch Netgear GS108T with Static IP Address 192.168.1.4.

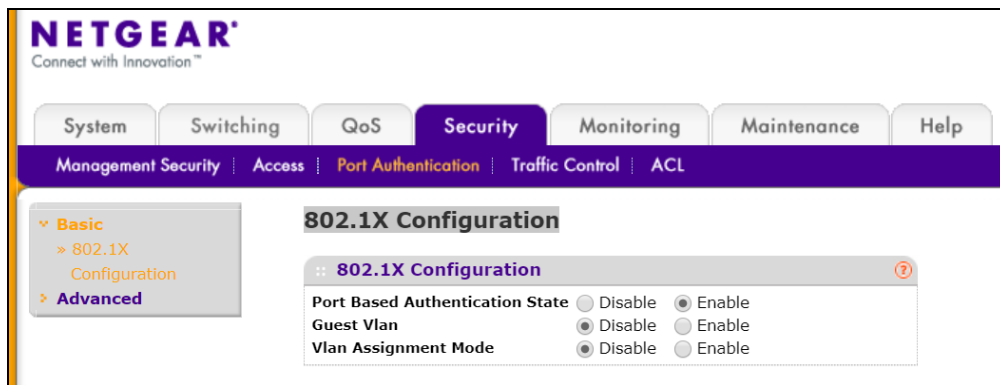
1. For Port Authentication: **Security > Port Authentication > Advanced > Port Authentication:**
  - a. Set **Port Control** to **Auto** to indicate the ports that will authenticate the connection using RADIUS Server.
  - b. Set **Port Control** to **Authorized** for the ports that will not be restricted.

**Figure 22: Port Authentication configuration**



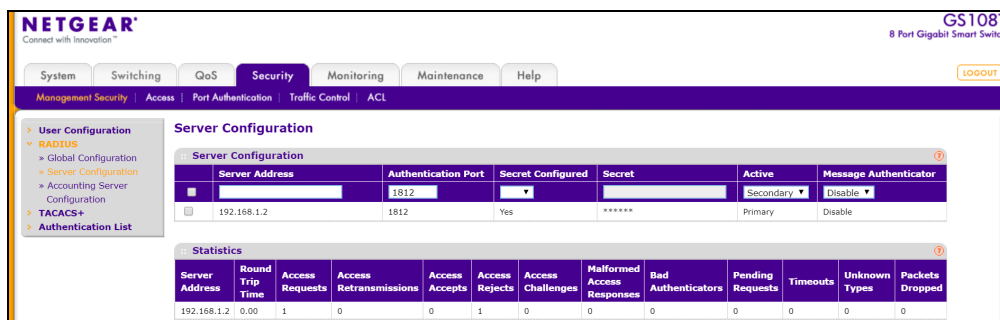
2. For 802.1X Configuration: **Security > Port Authentication > Basic > 802.1X Configuration**, enable 802.1X for Port Based Authentication.

**Figure 23: 802.1X configuration**



3. For RADIUS Server configuration: **Security > Management Security > RADIUS Server Configuration**, add a configuration for the RADIUS server, indicating the shared secret defined in the NPS RADIUS Client created for this connection.

**Figure 24: RADIUS Server configuration**



- For Authentication List: **Security > Management Security > Authentication List**, edit the current “defaultList” to set RADIUS as the first authenticator.

Figure 25: Authentication List configuration

List Name	1	2	3
<input type="checkbox"/> defaultList	RADIUS	Local	None

## 8.5.5 Wireless Connection

Wi-Fi access point Netgear R6220 with Static IP Address 192.168.1.3.

For Restricted Wireless Network: **Basic > Wireless**, choose one of the wireless networks for the 802.1X authentication (2.4 GHz in this example).

- Security Options: Set WPA/WPA2 Enterprise.
- Security Options details: Set WPA2 [AES] (it also works with WPA).
- Specify the RADIUS Server's IP address and set the shared secret defined in the NPS RADIUS Client created for this connection.

Figure 26: Wireless Network configuration

Wireless Network (2.4GHz b/g/n)

Name (SSID): NETGEAR45

Channel: Auto

Mode: Up to 300 Mbps

Enable SSID Broadcast

Enable 20/40 MHz Coexistence

Security Options

None

WPA2-PSK [AES]

WPA-PSK [TKIP] + WPA2-PSK [AES]

WPA/WPA2 Enterprise

Security Options (WPA/WPA2 Enterprise)

Encryption mode: WPA2 [AES]

Group Key Update Interval: 3600 (Seconds)

RADIUS Server IP Address: 192.168.1.2

RADIUS server Port: 1812

Shared Key: \*\*\*\*\*

## 8.6 Glossary

**AAA:** Authentication, Authorization, and Accounting.

**CA:** Certification Authority

**NPS:** Network Policy Server (this is the Microsoft implementation of the RADIUS standard)