Intel® Endpoint Management Assistant (Intel® EMA)

Release Notes

Intel® EMA Version: 1.5.1

Document update date: Wednesday, August 18, 2021

Legal Disclaimer

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 provides release-specific information for the current release of Intel® EMA.

Note: For the latest version of this document, please see https://downloadcenter.intel.com/download/28994?v=t).

1.1 Related Documentation

The following documentation is included as part of the Intel® EMA software release package:

Document (filename)	Description
Intel® EMA Quick Start Guide (Intel(R)_EMA_QuickStart_Guide.pdf)	Provides a simplified procedure for installing and configuring the Intel EMA server and deploying the Intel EMA agent for tutorial or proof-of-concept purposes in a small scale (i.e., laboratory) environment.
Intel® EMA Single/Distributed Server Installation and Maintenance Guide (Intel(R)_Single/Distributed_Server_ Installation_and_ Maintenance_Guide.pdf)	Provides complete installation, configuration, and maintenance instructions for implementing the Intel EMA server in a full scale production environment. A separate guide is provided for Single Server and Distributed Server installations.
Intel® EMA Administration and Usage Guide (Intel(R)_EMA_Admin_and_Usage_Guide.pdf)	Provides complete instructions for setting up and using Intel EMA to manage your endpoint systems.
Intel® EMA Web Deployment Guide for AWS/Azure/GCP (Intel(R)_EMA_Web_Deployment_Guide_for_ AWS/Azure/GCP.pdf)	Provides high-level conceptual information on how to deploy Intel EMA for a web-based services or cloud environment. A separate guide is provided for Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).
Intel® EMA API Guide	Provides detailed usage information for the Intel EMA Application Programming Interface (API).

(Intel(R)_EMA_API_Guide.pdf)	
Intel® EMA JavaScript Libraries Guide (Intel(R)_EMA_JavaScript_Libraries.pdf)	Provides detailed usage information for the JavaScript libraries included in Intel EMA.

1.1.1 Localized End User Documentation

Intel EMA user documentation is available in multiple languages. Available languages are German, Mexican Spanish, Brazilian Portuguese, Russian, and Simplified Chinese. Translated user documentation is available at the following links.

German

https://www.intel.com/content/www/de/de/support/articles/000055630/software/manageability-products.html

https://www.intel.com/content/www/de/de/support/articles/000058624/software/manageability-products.html

https://www.intel.com/content/www/de/de/support/articles/000058623/software/manageability-products.html

Mexican Spanish

https://www.intel.com/content/www/xl/es/support/articles/000055630/software/manageability-products.html

https://www.intel.com/content/www/xl/es/support/articles/000058624/software/manageability-products.html

https://www.intel.com/content/www/xl/es/support/articles/000058623/software/manageability-products.html

Brazilian Portuguese

https://www.intel.com/content/www/br/pt/support/articles/000055630/software/manageability-products.html

https://www.intel.com/content/www/br/pt/support/articles/000058624/software/manageability-products.html

https://www.intel.com/content/www/br/pt/support/articles/000058623/software/manageability-products.html

Russian

https://www.intel.com/content/www/ru/ru/support/articles/000055630/software/manageability-products.html

https://www.intel.com/content/www/ru/ru/support/articles/000058624/software/manageability-products.html

https://www.intel.com/content/www/ru/ru/support/articles/000058623/software/manageability-products.html

Simplified Chinese

https://www.intel.com/content/www/cn/zh/support/articles/000055630/software/manageability-products.html

https://www.intel.com/content/www/cn/zh/support/articles/000058624/software/manageability-products.html

https://www.intel.com/content/www/cn/zh/support/articles/000058623/software/manageability-products.html

1.1.2 Additional Intel AMT Information

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

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

2 What's New in this Release?

- A scaling performance issue introduced in v1.5.0 has been fixed.
- The version 2 (v2) APIs have been removed from this release of Intel EMA. The version 3 (v3) APIs will be removed in the next release of the Intel EMA API. Please upgrade any custom integration code you have created to use a new API version. We recommend you always update to the latest API version as soon as possible as older versions will be removed upon subsequent updates. If desired, you can use the "latest" API path (for example, GET /api/latest/802_1XSetups) to ensure you are always calling the latest API version in your code.
- The Intel AMT Discovery feature of Intel EMA has been removed.
- The JavaScript library ema_desktop.js has been updated in this release. The previous version of ema_desktop.js will no longer work with this release of Intel EMA. Please be sure to use the latest version of ema_desktop.js, available in this release of Intel EMA. See the *Intel® EMA JavaScript Libraries Guide* for more information.
- Intel EMA user documentation is now available in multiple languages. Available languages are German, Mexican Spanish, Brazilian Portuguese, Russian, and Simplified Chinese. See "Related Documentation" on page 1.
- 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-domains-and-trusts.
- Support of Denial of Service (DoS) IP limiting in both server services and agent. For details on applicable component server settings, see **Modifying Component Server Settings** in the *Intel® EMA Administration and Usage Guide*.
- Support for automatic renewals of 802.1x client certificates. For details on applicable component server settings, see **Modifying Component Server Settings** in the *Intel® EMA Administration and Usage Guide*.
- API support for User Consent. Previously, User Consent has been available through the Intel EMA user interface, but this release introduces API support for this capability. See the *Intel® EMA API Guide* for details.

  API support for Remote Secure Erase (RSE). Previously, RSE has been available through the Intel EMA user interface, but this release introduces API support for this capability. See **Remote Secure Erase** under **Key Concepts** in the *Intel® EMA Administration and Usage Guide*, or see the *Intel® EMA API Guide* for details on applicable API calls.
- New ability to adjust or disable agent automatic update. This is helpful when updating the Intel EMA server in an environment with a large number of endpoints that will attempt to update. For details on applicable component server settings, see **Modifying Component Server Settings** in the *Intel® EMA Administration and*

Usage Guide.

- The Endpoints page has been modified to not load endpoint summary data automatically, but rather allow users to choose whether endpoint summary data is collected and displayed. Users can also search for a particular endpoint before loading data for all endpoints.
- Some database table and column names have been changed in this release (for example NodeHistory is now EndpointHistory) Any external (non Intel EMA) references will need to be updated).
- Intel EMA has been enhanced to provide some migrations for Denial of Service (DoS) attacks, including Per-IP Rate Limiting, Per-IP Connection Count Limiting, and Unauthenticated TCP TLS Idle Connection Timeout. These mitigations are applied to specific ports on the Intel EMA component servers (i.e., Swarm Server, Ajax Server, etc.), and are user configurable via a new suite of component server settings, available on the Intel EMA UI's Settings tab.
- The Intel EMA Agent version numbering has been changed to 1.x.x (formerly 0.x.x).
- The Intel EMA Agent now reconnects to the Swarm Server after disconnect at a random interval to prevent all agents from attempting reconnection at the same time. As a result, it can take several minutes for all agents to reconnect.
- The Intel AMT tab is now labeled Hardware Manageability tab, with revisions to support future Intel platforms.
- Support for clipboard paste from console to endpoint.
- Upper limit for storage of USBR images has been increased to 500 GB.
- OpenSSL version updated to the latest version.

2.1 Upgrading from v1.3.1 to v1.3.2 or later

A fresh install is recommended when upgrading from Intel EMA 1.3.1. If upgrading from Intel EMA 1.3.1, please be aware of the following.

- Due to a known issue, the Intel EMA 1.3.1 agent will not automatically upgrade to the new version as it normally would. The Intel EMA agent must be reinstalled with the 1.3.2 or later version to restore normal operations.
- The FileActions and Installer processes included in Intel EMA 1.3.1 are no longer included as part of Intel EMA and will fail to start after upgrading to v1.3.2 or later. Use the Platform Manager to stop and remove these two items from the Runtime and Storage tabs.
- If you created user groups in Intel EMA version 1.3.1, you will notice that your existing user group names are displayed differently in the current version's user interface. Starting with version 1.3.2, user group names now include the group's rights (Execute or View) appended at the end. See examples below:

  ```
  MyGroupName@@@@Execute
  ```

  ```
  MyOtherGroupName@@@@View
  ```

- If you are using a custom user or system account to run Intel EMA services under, you will need to reset that account again after the upgrade and then reboot to restart the services under that account.

3 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†)
- 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

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

4 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 3.
    - 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.

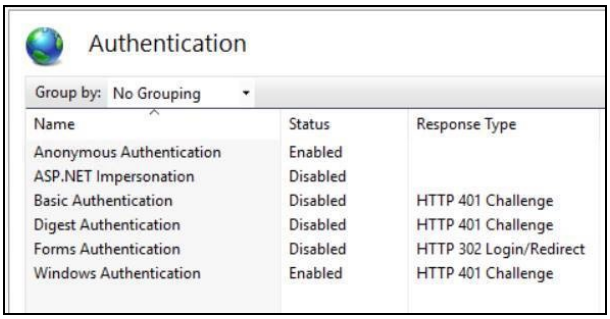
    Notes:

    - 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 3.
    - 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.

- **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.

- **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 archecture 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.
TCP	8092	Port on which Ajax component server listens for internal component-to-component communication. This port number is the default, and can be changed in the Server Settings page.
TCP	8093	Port on which Swarmcomponent server listens for internal component-to-component communication. This port number is the default, and can be changed in the Server Settingspage.
TCP	8094	Port on which Manageability component server listens for internal component-to-component communication. This port number is the default, and can be changed in the Server Settings page.

4.1 Agent Prerequisites

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

- **Operating System:** Intel® EMA Agent is officially supported on Microsoft Windows 7 and 10, both 32bit and 64bit operating systems.
- **Note:** Windows 7 is supported on Intel AMT 11.8 systems only and will be no longer be supported after Intel AMT 16 is released.
- **Firewall:** When Intel EMA Agent is installed, it will set up the following Windows Firewall in-bound rules for the installed agent binary process. If you are using a different firewall, make sure that the following in-bound rules are set for the installed agent binary process:
  - Peer-to-peer traffic: UDP with local port at 16990, any IP for local and remote addresses, and edge traversal blocked.
  - Peer-to-peer traffic: TCP with local port at 16990, any IP for local and remote addresses, and edge traversal blocked.

- Local loopback management traffic: TCP with local port at 16991, 127.0.0.1 for local and remote addresses, and edge traversal blocked.

- **Intel® Active Management Technology (Intel® AMT):** Intel EMA only supports Intel® AMT 11.8 and higher. Only required for Out-of-band endpoint management.
  The following table lists the minimum Intel AMT versions required on endpoints to use USBR over CIRA.

Intel AMT Version	Build Number
Intel AMT 11.8	all
Intel AMT 12	12.0.70.1607 or later
Intel AMT 14	14.0.45.1341 or later
Intel AMT 15	all

  For more information about USBR, see section 1.

5 Known Issues and Limitations

CIRA Connection Compatibility	Intel vPro® systems updated with Intel® AMT 12 manageability engine firmware v12.0.45.1509 or higher require Intel® EMA 1.3.2.1 or later to ensure CIRA connection compatibility. • Recommend upgrading to Intel EMA 1.3.2.1 or later as soon as possible • If you have existing Intel AMT 12 systems provisioned via CIRA and they have been upgraded to Intel AMT FW v12.0.47.1524 or higher, those systems will need to be unprovisioned/reprovisioned via Intel EMA after the upgrade. If Intel AMT auto setup is configured in the Intel EMA endpoint group, reprovisioning can also be triggered to happen on all endpoints in that endpoint group automatedly by making any profile change (for example changing the description). • If CIRA does not connect when the endpoint is powered down or if the OS is not running, check the Intel AMT wireless profile in Intel EMA. When the endpoint OS is down, Intel AMT's CIRA relies on the Intel AMT WiFi profile in Intel EMA for its connection settings. Out-of-band CIRA connection issues can often be corrected by selecting Counter mode CBC MAC Protocol (CCMP) for the Security Type in the Intel AMT WiFi profile. Also, check that the wireless router's or hotspot's SSID is broadcasting and not hidden. Lastly, if the endpoint is a laptop, ensure its power supply is plugged in. For more information, see "Creating a New WiFi Profile" in the *Intel® EMA Administration and Usage Guide*.
Resource Conflict error when booting endpoint to image via USBR	If you attempt to boot an endpoint that is powered off to a mounted image via USBR (using the "Boot to this Image" link on the endpoint's details page), you will see a "Resource Conflict" error message. **To fix:** • Power on the endpoint, then use the "Boot to this Image" link to boot the endpoint to the mounted image. -OR- • Use the "Power up to IDE-R Image" feature under Power Actions on the Hardware Manageability tab.
Intel® EMA Agent	• To uninstall the service, or to install/update the service on top of an existing installation, you must use an Intel® EMA Agent installer with the same architecture type (32-bit service or 64-bit service) as the existing Intel EMA Agent. • When you download the endpoint group policy file for the agent, it may fail if you are using Internet Explorer on Windows Server. The reason is that the policy file is not signed and Internet Explorer on Windows Server has Enhanced Security enabled by default. You can use a different web browser or change the security settings for Internet Explorer.

Internet Explorer settings when Intel® EMA is installed under domain/Windows authentication mode	• For the domain/Windows authentication to work correctly, the Intel EMA website should be recognized as in the Local Intranet zone. You can verify the zone by right-clicking the Intel® EMA web page and then choosing Properties. • Some users may have "Display intranet sites in Compatibility View" enabled in the Compatibility View Settings of Internet Explorer. This setting must be disabled (unchecked); otherwise, Intel EMA website will not work correctly.
Data refreshing	The website does not automatically update the displayed data. The data update is triggered only after you perform certain actions or when you refresh the web page.
Intel® AMT Provisioning	• If Intel AMT on the endpoint is setup/provisioned by some other tool (i.e., Intel EMA database does not have any record of this setup), then Intel EMA cannot manage this Intel AMT. The user needs to clear up / unprovision this endpoint first and then use Intel EMA to do the setup. • Before you use Intel EMA to un-provision an endpoint, check the current provisioned control mode shown at the endpoint's detail information. It needs to be in either Client Control Mode or Admin Control Mode for un-provisioning to work. If it is in provisioned complete but not in Client Control Mode or Admin Control Mode, please restart the endpoint first for Intel EMA to get the correct status. • Intel AMT CILA (Client Initiated Local Access) is not supported/set-up by Intel EMA. • The Intel EMA UI states that the character limit for passwords is 32 characters, however the actual limit is 31 characters.
Intel® AMT Profile	• A profile can only be used with Intel AMT auto-setup. It cannot be used with on-demand setup. • A profile cannot be removed if the profile is used by an endpoint group or is used by any endpoint for provisioning. • If an Intel AMT profile was used for auto-provisioning but auto-provisioning is now disabled, the profile cannot be deleted. In order to delete this profile, you must first re-enable auto provisioning and select a different profile. The reason is that, even though auto-provisioning was disabled for the endpoint group, the actual endpoints in this group are still using the profile. Therefore, this profile cannot be deleted until the endpoints are switched to a different profile. • 802.1X: Currently, Intel EMA supports only EAP-TLS as the authentication protocol.
Endpoints' batch actions	• View Desktops: This feature is using 1 websocket connection per endpoint. If you are using Internet Explorer, Internet Explorer has limit for the maximum number of the concurrent websockets, which is 6. Choose no more than 6 endpoints if you are using Internet Explorer.

	• View Desktops: Currently, when the user adjusts the “screen per row” slider, the remote in-band KVM is re-established to all the target endpoints. If the endpoint group policy "User consent for in-band KVM" is enabled, the user(s) must consent again. • On the Managed Endpoints tab, when logged in as an Endpoint Group User or Endpoint Group Creator role, if you select multiple endpoints and then click the **Manage this endpoint** drop-dwon menu, you may see actions that you cannot perform. The Intel EMA UI does not check user permissions for which actions to display in this menu when multiple endpoints are selected. However the underlying code will prevent unauthorized users from performing any actions for which they do not have permission.
Endpoint’s power status	The power status is not guaranteed to be correct. Correct power status is guaranteed only when the endpoint is setup/provisioned under Intel AMT CIRA.
Cross-origin requests blocked for in-band KVM, terminal, files, processes, and WMI tabs	The URL you used to access Intel EMA web site needs to match the URL used during Intel EMA server installation. If they do not match, you will get an alert pop-up window right after you log in to inform you about this. If you choose to continue, those features mentioned above may not work.
Each endpoint’s in-band KVM	• When the target endpoint displays DPI value changes, the current user on the endpoint must sign out and sign in again so that Intel EMA Agent can get the current display resolution. This limitation is shared by many Windows applications. • In the latest Windows 7, when you change the display resolution, Windows auto-changes the DPI value also. In this case, the above limitation also applies. • Windows 7 does not support different DPI values for multiple displays. To support Windows 7, if the endpoint has multiple displays, all displays must have the same DPI setting as the primary display for Intel EMA Agent to get current resolution for other displays. • On the Chrome browser, the in-band KVM may appear black or has a block of black region. It will be updated when that black region gets the next screen fresh.
Each endpoint’s out-of-band (Intel® AMT) KVM	• Laptop device/endpoint: Be sure to open the lid of the laptop to ensure KVM functions correctly. • Desktop and headless devices/endpoints: Be sure to plug a monitor in to desktop or headless endpoints, to ensure KVM functions correctly. • Device emulator: You may run a device emulator (High Definition Multimedia Interface - HDMI or other) to have the system function as if there’s a monitor attached.
Each endpoint’s file tab	Currently, for the endpoint group policy, you must enable both Files and KVM policies. Otherwise, the Intel EMA Agent will reject this request.
Endpoints’ remote file search	• Search conditions will accept only characters from a to z, A to Z, 0

	to 9, *, and ?. All other characters will be filtered out. • The maximum returned search result is about 20,000 characters. Any results after this limit will be truncated. Therefore, the user may need to use a more-detailed search condition to avoid a long search result. • This depends on Windows indexing. Windows finds only those files in “indexed” locations. • On the Managed Endpoints page, under **Action > Remote File Search**, entering a file extension (i.e., `filename.ext`) is not supported. To search for a remote file, enter the filename without any extension (do not include a ".*" either), and the search will return all files matching that filename. The issue is that the "." character is not currently supported, so any filename that includes the "." will fail.
Endpoints with statically assigned IP addresses	• Intel AMT CIRA’s environment detection does not work with endpoints that have been configured with static IP addresses. • Endpoints with static IP addresses are not displayed in Intel AMT Discovery. • We recommend that you use dynamic IP addressing for your endpoints.
Ctrl-C in terminal window causes agent to stop working	In a terminal window session with an endpoint, if you send a command to show one screen at a time (for example, ipconfig /all | more) and then press **Ctrl-C**, the agent will stop working. To fix this, you must reboot the managed endpoint. Simply stopping and restarting the agent service will not work.
Terminal tab	• Only ASCII text-based commands are supported. Some BIOS's that use UTF8 will be displayed incorrectly. • The terminal tab displays only the last 80 by 25 characters. Windows command console also has a display limit; however, Windows command console's limit is much longer than the current limit here. • For in-band terminal connections, if the endpoint is running the latest Windows 10, the terminal window may not display correctly. • The Intel AMT Terminal (Serial-Over-LAN or SOL) feature requires that you use another tool to reboot the endpoint to BIOS with SOL enabled in BIOS.
Slow response updating endpoint data in Internet Exporer	When running Intel EMA in Internet Explorer, endpoint data updates can take over two minutes when the total number of managed endpoints exceeds 50K endpoints.
Port Not Available Error When Using endpointOOBOperations/Single APIs	For endpoint OOB operations (for example, Intel AMT power operations), two versions of each API are provided: one for single endpoint operations, and one for multiple endpoint operations. If you use the single APIs concurrently on a large number of endpoints (greater than 100K, depending on other processes that may be using ports on the Intel EMA server), you may get a “Port Not Available” error. We recommend using the end-

	pointOOBOperations/Multiple APIs for concurrent operations on large numbers of endpoints.
Failover for machine hosting Web server and Ajax server components in a distributed server architecture	In a distributed server architecture environment, the Intel EMA Web server and Ajax server components work together to handle traffic on port 443. Therefore, the load balancer health monitoring rule (which is based on port only) will not detect when only one of these components is down. However, it will detect when the server machine as a whole is down (i.e., both Web and Ajax compoents are down) and failover to another healthy machine.
Intel EMA API token expiration while using Intel EMA website UI	Once you login to the Intel EMA website UI, Intel EMA uses that API token for subsequent API requests. The token's default expiration time is 60 minutes. Intel EMA does not automatically refresh the token, even if you are continually using the Intel EMA website UI.
Visual and performance issues when using Hardware Manageability tab	The Hardware Manageability tab in Intel EMA makes use of Intel Manageability Command (Intel MC) to provide the functionality available on this tab. Due to known issues with Intel MC, depending on the browser you use to open Intel EMA, you may notice some cosmetic issues with the visual display and UI functionality when using the features of the Intel Hardware Manageability tab. Refreshing the page often fixes some of the display issues.
After upgrade to v1.3.3, the Intel Hardware Manageability tab may still call previous Intel MC version	After upgrading Intel EMA to version 1.3.3, you may notice that the version of Intel Manageability Commander (Intel MC) that is called when using the Intel Hardware Manageability tab of Intel EMA is not the latest Intel MC version (2.1). To correct this, clear your browser's cache, then refresh the Intel Hardware Manageability tab page in the browser. The correct version of Intel MC (v2.1) should now be called from the Intel Hardware Manageability tab.
Remote connection to endpoint dropped when restarting the endpoint	When restarting a managed endpoint over a remote connection to the endpoint's Intel AMT, you may see Intel EMA's TCP connection to the endpoint drop as the endpoint restarts. This is due to temporary link loss as the endpoint transitions from the Intel Management Engine (Intel ME) to the OS network stack, during which Intel EMA retries to send TCP packets to the transitioning endpoint. A Microsoft network stack configuration TcpMaxRetransmissions allows only 5 TCP retransmission attempts (approximately 3 seconds) by default. Newer OS's (19H1 and above) have a slower transition from the Intel ME to the OS network stack, and as a result Intel EMA exceeds the maximum number of TCP retransmission attempts and the remote connection is dropped. **To fix:** You can avoid this issue by modifying the Microsoft registry key in the Windows OS on your Intel EMA server(s) to set the TcpMaxRetransmissions value to 7 or higher. This will allow Intel EMA enough retries to keep the remote connection established as the endpoint transitions to the OS network stack. Follow the steps below. 1. Open the Registry Editor (regedit.exe) 2. Browse to "HKEY_LOCAL_MACHINE\Sys-

	tem\CurrentControlSet\Services\Tcpip\Parameters” 3. Find or create the following: a. Value Name: TcpMaxDataRetransmissions b. Value Type: REG_DWORD c. Value Data: 7 For additional information, see the following Microsoft article: https://support.microsoft.com/en-us/help/170359/how-to-modify-the-tcp-ip-maximum-retransmission-time-out
KVM disconnects during endpoint power state change	If you experience a disconnect during a power state change when using out of band KVM, wait a few seconds and attempt to reconnect.
Image mount via USBR fails	If an attempt to mount an image to a managed endpoint via USBR fails, the cause may be that the Intel AMT redirection port was not enabled during provisioning. Use the Harware Manageability tab, available by selecting **Endpoints** on the navigation bar, to enable the redirection port on that endpoint.
Booting an endpoint to a mounted image via USBR fails	Check the format of your image file. Ensure the format is CDFS, not UDF. There is a current known issue with Intel AMT booting some UDF formatted images via USBR. Sometimes UDF formatted images may not boot or may not boot fully. We recommend using CDFS formatted images until this issue is resolved.
Importing PKI certificate fails on Windows Server 2012 or 2016	If you have installed the Intel EMA Server on a machine running Windows Server 2012 or 2016 (earlier than build 1709), uploading a certificate into Intel EMA will fail if the certificate PFX file used encryption “AES256-SHA256". An error about an invalid password will be displayed, even though a valid password is provided. This is a Windows issue in which Windows itself does support PFX files created using this encryption. This issue is fixed starting with Windows Server 2016 build 1709 and later. https://github.com/dsccommunity/CertificateDsc/pull/154/files **To fix:** 1. Install the PFX file on a system that supports the PFX file with encryption “AES256-SHA256" (for example, Windows 10 desktop). To do this, double click the PFX file to launch the Certificate Import Wizard. By default it will install to the currently logged-in user's personal certificate store. Be sure to select **Mark this key as exportable** and **Include all extended properties**. 2. Open Microsoft Management Console for current user certificates. 3. Right-click on the certificate that was just installed, then select **All Tasks> Export...**. This will open the Certificate Export Wizard. 4. In the wizard, select **Yes, export the private key** and click **Next**. 5. Select **Personal Information Exchange (.PFX)** and select **Include all certificates in path**, **Export all extended properties**, and

	Enable certificate privacy. If desired, select **Delete the private key if successful** (do this if you want to remove the certificate and key from this intermediate system). Click **Next**. 6. On the security screen select the **Encryption** "TripleDES-SHA1". This is basis of the issue: older versions of Windows do not support PFX files with "AES256-SHA256". This encryption is not for the actual certificate , but rather it is used along with the password provided on this screen to protect the private key associated with the certificate when it is exported out to the PFX file format. 7. Finish the export wizard screens to create a new PFX file. This new PFX file can be successfully used on the older Windows system on which you installed the Intel EMA server.
In-band KVM paste from clipboard results in unexpected characters or case	When attempting to paste plain text from the clipboard of the Intel EMA console system (i.e., the clipboard of the computer running the Intel EMA web-based UI) to an endpoint via KVM, you may notice unexpected case or capitalization in the pasted output on the target endpoint. This is consistent with other remote desktop applications' behavior. For more information, see the following link from Microsoft: https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/caps-lock-key-status-not-synced-to-client Further, depending on the OS language/locale of the target endpoint, unexpected characters may be pasted. Only US English keyboard character codes are supported. If the endpoint's language/locale is not US English, unpredictable characters may be pasted on the endpoint. **To fix (capitalization issue only):** • Ensure that the Caps Lock is OFF on the target endpoint before pasting. If you pressed Caps Locks during a KVM session to that endpoint, be sure to press Caps Lock again before exiting the KVM session to clear (turn off) the Caps Lock on the target. Otherwise Caps Lock will remain ON on the endpoint, and when you paste to that endpoint, the pasted text will behave accordingly (lower case as all caps, and vice versa).
Event 7030 Agent Background Service Error	The following error message may be seen in the Windows System log. This is expected and is not a cause for concern. This nuisance error will be corrected in a future release. "The Intel(R) EMA Agent background service service is marked as an interactive service. However, the system is configured to now allow interactive services. This service may not function properly."
CloudWatch issue with AWS	If used or enabled on AWS instances of Intel EMA, CloudWatch can prevent the Swarm server process from restarting due to files being kept open or in use. **To fix:** Disable CloudWatch or configure it to ignore Intel EMA processes and associated files.

Port conflict issues between Intel EMA component servers and Splunk application	Be aware that in a distributed server installation, the application Splunk can cause conflict issues with the component server communication over the default management port TCP 8089.
Do not use browser's Back button when running Intel EMA web based UI	Using the browser's Back button when running the Intel EMA web based UI can but the UI in an unpredictable state. Use the UI's navigation elements to move within the UI.