



# **Ivanti EPMM 11.4.0.0. - 11.12.0.0 System Manager Guide**

**November 2023**

# Revision history

For the complete revision history, see the [online version](#) of this document.

# Contents

---

<b>Revision history</b>	<b>2</b>
<b>Introducing System Manager</b>	<b>5</b>
System Manager Overview	5
Starting System Manager	6
Logging into the System Manager	7
Logging into the System Manager with user ID and password	7
System Manager Workspace	8
<b>System Settings</b>	<b>13</b>
Settings overview	13
Network: Interfaces	15
Network: Routes	18
DNS and Hostname	19
Static Hosts	20
Date and Time (NTP)	21
CLI	22
Data Export: Splunk	23
Data Export: SysLog	26
Data Export: Reporting Database	30
SNMP	31
Email Settings	36
Port Settings	38
Data Purge	43
<b>Security Settings</b>	<b>47</b>
Identity Source: Password Policy	47
Certificate Mgmt	60
Access Control Lists: Network Services	69
Access Control Lists: ACLs	70
Access Control Lists: Portal ACLs	73
Advanced: Host Header Validation	74
Advanced: HSTS	75
Advanced: Incoming SSL Configuration	77
Advanced: Outgoing SSL Configuration	82
Advanced: ModSecurity	90
Advanced: SAML	92
Advanced: Trusted Front End	102
Advanced: Portal Authentication	104
Advanced: SSH Configuration	116
<b>Maintenance Settings</b>	<b>119</b>
Maintenance overview	119
Software updates	120
Export configuration	120

---

---

Import a configuration .....	120
Clear configuration .....	121
System Storage .....	121
Reboot .....	125
System backup .....	125
<b>Troubleshooting .....</b>	<b>139</b>
Troubleshooting overview .....	139
Working with logs .....	140
Network monitor .....	146
Service diagnosis .....	147
System monitor .....	148
Queue Activation .....	151
In-Memory Queue Monitor .....	151
<b>Upgrading Ivanti EPMM Releases .....</b>	<b>153</b>
Upgrading overview .....	153
Upgrade planning notes .....	153
Upgrade Ivanti EPMM using System Manager .....	156
Updating Ivanti EPMM using the CLI .....	159
Ivanti EPMM OS and platform updates .....	161
Advanced: SAML .....	163

# Introducing System Manager

## System Manager Overview

After installing Ivanti EPMM, administrators have access to the following web portal tools:

- **System Manager:** for performing most configuration tasks, including:
  - Configuring Ivanti EPMM
  - Managing network settings
  - Managing Ivanti EPMM within your infrastructure
  - Upgrading Ivanti EPMM
  - Troubleshooting and maintenance
- **Admin Portal:** for performing most common administrative tasks.

Refer to your *Ivanti EPMM Device Management Guide* for information on using the Admin Portal.

- Ivanti recommends to allow HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for EPMM server management and must have strictly controlled access.
- The [Ivanti documentation site](#) provides access to access Ivanti product documentation.

## Terminology

The following terminology is used in this document.

- **MICS:** MobileIron Configuration Service (the service that supports System Manager)
- **MIFS:** MobileIron File Service (the service that supports the rest of Ivanti EPMM)

---

## Starting System Manager

You can start System Manager two ways:

- ["Starting System Manager using the URL" below](#)
- ["Starting System Manager from the Admin Portal" below](#)

Ivanti recommends to allow HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for EPMM server management and must have strictly controlled access.

## Starting System Manager using the URL

### Procedure

To start System Manager using the System Manager URL:

1. Open a supported browser.

Refer to the latest release notes for information on supported and compatible browsers.

2. Enter your Ivanti EPMM URL in the browser to open the System Manager log in screen.

For example: `https://<EPMM_fully_qualified_hostname>:8443/mics`

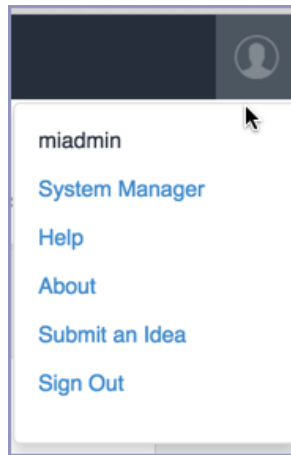
## Starting System Manager from the Admin Portal

### Procedure

To start System Manager from the Admin Portal:

1. Log into the Admin Portal.
2. Click on the person icon at the top right of the Admin Portal page.

- 
3. Select **System Manager** from the menu to open the System Manager workspace.



The System Manager login screen displays.

## Logging into the System Manager

When first setting up Ivanti EPMM, a system administrator determines which login methods are allowed for the System Manager.

- ["Logging into the System Manager with user ID and password" below](#)
- [" Logging into the System Manager with a smart card " on the next page](#)

### Related topics

- ["Advanced: Portal Authentication" on page 104](#)
- ["Identity Source: Local Users" on page 57](#)

## Logging into the System Manager with user ID and password

If supported by your system administrator, you can login to the System Manager with a user ID and password. Refer to ["Advanced: Portal Authentication" on page 104](#) for information on setting up this authentication method. The user ID is case-sensitive and must be either:

- The user ID created during the initial setup of Ivanti EPMM
- The user ID created in the System Manager under **Security > Identity Source > Local Users**.

---

## Procedure

1. In the web browser displaying the System Manager login screen, enter the user ID and password of a System Manager user.
2. Click **SIGN IN** to open the System Manager workspace.

## Logging into the System Manager with a smart card

If supported by your system administrator, you can login to the System Manager on a desktop computer using an identity certificate on a smart card. Refer to ["Advanced: Portal Authentication" on page 104](#) for information on setting up this authentication method. This user must be a local user created in the System Manager under **Security > Identity Source > Local Users**.



This authentication method is supported only on desktop computers. It is not supported on mobile devices. Also, it is not supported with Firefox.

---

## Procedure

1. Attach your smart card reader with your smart card to a USB port on the desktop computer. If your computer has a built-in smart card reader, insert your smart card.
2. Go to the URL of the System Manager at `https://<fully_qualified_hostname>:8443/mics`
3. If you are not logged in, select **Sign In With Certificate**. A prompt appears to select your certificate.
4. Select the certificate from the smart card.
5. If prompted, enter the password of the private key of the identity certificate on your smart card. The System Manager workspace displays.

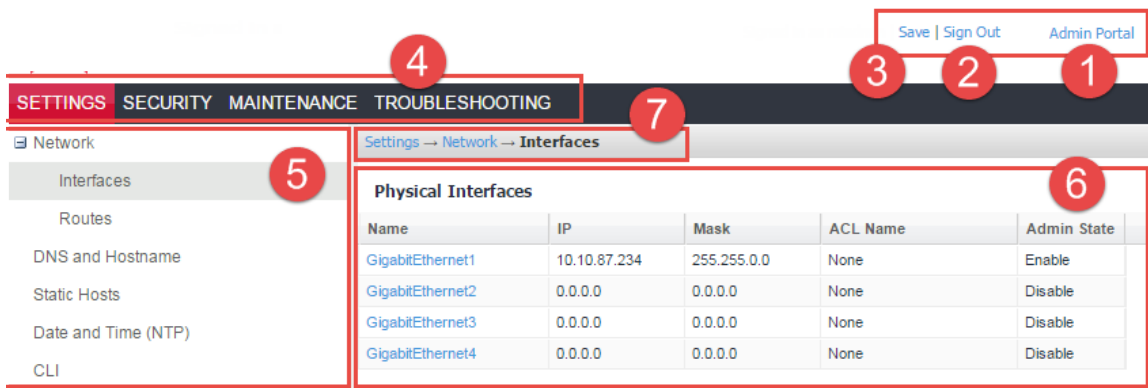
## System Manager Workspace

System Manager is a web-based portal where you can perform most configuration tasks. When you log into System Manager, you are presented with the System Manager workspace, which has the following components (the number listed below correspond to the numbers in ["System Manager workspace" on the next page](#)):



1. **Admin Portal link:** opens the Admin Portal.
2. **Sign Out button:** exits System Manager and automatically retain (but does not save) current settings, however, rebooting Ivanti EPMM without saving settings returns Ivanti EPMM to its previously-saved configuration.
3. **Save button:** saves current settings.
4. **Menu tabs:** lists the top-level System Manager functionality.
5. **Menu items pane:** lists each item associated with the selected menu.
6. **Menu item details pane:** lists the detailed functionality and options for the selected menu item.
7. **Menu item(s) breadcrumbs:** provides a menu > menu item path.

FIGURE 1. SYSTEM MANAGER WORKSPACE



## System Manager menus

The following table describes the top-level menus, menu items associated with each menu, and the tasks of each menu item.

TABLE 1. SYSTEM MANAGER MENUS

Menu Item	Task
<b>Settings Menu</b>	
Network > Interfaces	<ul style="list-style-type: none"> <li>• Change physical interface settings</li> <li>• Add VLAN interfaces</li> <li>• Change VLAN interfaces</li> </ul>

**TABLE 1. SYSTEM MANAGER MENUS (CONT.)**

Menu Item	Task
Network > Routes	<ul style="list-style-type: none"><li>• Change the default gateway</li><li>• Route through different gateways</li></ul>
DNS and Hostname	Change DNS servers
Static Hosts	Edit the host list for Ivanti EPMM
Date and Time (NTP)	Change the time source used by Ivanti EPMM
CLI	<ul style="list-style-type: none"><li>• Change the Enable Secret set during installation</li><li>• Enable/Disable ssh access</li><li>• Change ssh settings</li></ul>
Data Export > Splunk Indexer	Configure a Splunk indexer
Data Export > Splunk Data	Configure the data to export to Splunk
Data Export > Syslog Servers	Configure syslog servers.
Data Export > SysLog Data	Configure the data to export to Syslog servers.
Data Export > Reporting Database	Configure the authentication token for the Reporting Database and the data to export
Log Upload	Upload log files to an external server.
SNMP	Configure SNMP servers
Email Settings	Configure SMTP settings for communication between Ivanti EPMM and devices
Port Settings	Change default port configuration for Ivanti EPMM
Data Purge	Configure automated data purging
Services	Enable/Disable Ivanti EPMM services
<b>Security Menu</b>	
Identity Source > Local Users	Create, delete, and manage local users for System Manager.
Identity Source > Password Policy	Create, edit, and restore default values for password in the System Manager.
Certificate Mgmt	View and manage certificates for: <ul style="list-style-type: none"><li>• Portal HTTPS</li></ul>

**TABLE 1. SYSTEM MANAGER MENUS (CONT.)**

Menu Item	Task
	<ul style="list-style-type: none"><li>• Client TLS</li><li>• iOS Enrollment</li><li>• Certificate pinning requests</li></ul>
Access Control Lists > Networks & Hosts	Create and manage entries for networks and hosts
Access Control Lists > Network Services	Create and manage entries for network services
Access Control Lists > ACLs	Compile access control lists
Access Control Lists > Portal ACLs	Compile access control lists for specific Ivanti EPMM components
Advanced > Host Header Validation	Enhance security of incoming HTTP traffic in Ivanti EPMM, by validating HTTP host headers
Advanced > HSTS	HSTS provides an additional layer of security for HTTPS, reducing the ability to intercept requests and responses between a user and a web application server.
Advanced > Incoming SSL Configuration	Select protocols and cipher suites other than the defaults for incoming SSL/TLS connections
Advanced > ModSecurity	Configure protection against certain types of future public security vulnerabilities
Advanced > Outgoing SSL Configuration	Select protocols and cipher suites other than the defaults for outgoing SSL/TLS connections.
Advanced > SAML	Allows local administrator users to use single-sign on for the Admin Portal and Self-Service User Portal.
Advanced > Trusted Front End	Set up a Trusted Front End for communication from devices to Ivanti EPMM.
Advanced > Portal Authentication	Select whether device users authenticate to the self-service user portal, Admin Portal, and System Manager with a password, certificate, or both.
Advanced > SSH Configuration	Configures ciphers, key exchange algorithms and hmacs.
<b>Maintenance Menu</b>	

**TABLE 1. SYSTEM MANAGER MENUS (CONT.)**

Menu Item	Task
Software Updates	Update the following information with Ivanti EPMM upgrade: device operating system, version information, platform type
Self Diagnosis	Automates maintenance by providing rapid responses to fixing important issues and reducing the need for patch releases.
Export Configuration	Export Ivanti Server configuration settings to XML format.
Import Configuration	Import an Ivanti Server configuration from a local XML file or FTP site.
Clear Configuration	Clear unsaved configuration settings and return to the default configuration.
System Storage	Monitor disk storage availability.
Reboot	Clear current configuration settings and restart all server modules.
System Backup	Back up system configurations.
Optimize Database	Optimize Ivanti EPMM database performance by cleaning up fragmentation in the database
<b>Troubleshooting Menu</b>	
Logs	Use logs to debug the system.
Network Monitor	Produces a TCP dump for one of the Ivanti Server physical interfaces.
Service Diagnosis	Check the health of multiple services, such as MapQuest, DNS, NTP, and Email.
System Monitor	Monitor Ivanti EPMM performance in log files that contain performance information about CPU usage, memory usage, threads, tomcat performance, database performance, and muscle logs.
Queue Activation	Provides data about Queue Activation that is useful to Ivanti Technical Support.
In-Memory Queue Monitor	Provides Ivanti Technical Support with information about tasks in the queue in your Ivanti EPMM memory.

# System Settings

- [Settings overview](#)
- [Network: Interfaces](#)
- [Network: Routes](#)
- [DNS and Hostname](#)
- [Static Hosts](#)
- [Date and Time \(NTP\)](#)
- [CLI](#)
- [Data Export: Splunk](#)
- [Data Export: SysLog](#)
- [Data Export: Reporting Database](#)
- [Log Upload](#)
- [SNMP](#)
- [Email Settings](#)
- [Port Settings](#)
- [Data Purge](#)

## Settings overview

System Manager **Settings** contains menu items for configuring Ivanti EPMM. The following table summarizes the tasks associated with each menu item.

Ivanti recommends to allow HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for EPMM server management and must have strictly controlled access.

**TABLE 2.** SYSTEM MANAGER SETTINGS MENU ITEMS

Settings Menu	Task
Network > Interfaces	<ul style="list-style-type: none"> <li>• Change physical interface settings</li> <li>• Add VLAN interfaces</li> <li>• Change VLAN interfaces</li> </ul>
Network > Routes	<ul style="list-style-type: none"> <li>• Change the default gateway</li> <li>• Route through different gateways</li> </ul>
DNS and Hostname	Change DNS server details
Static Hosts	Add, edit, and delete the host list for Ivanti EPMM
Date and Time (NTP)	Change the time source used by Ivanti EPMM
CLI	<ul style="list-style-type: none"> <li>• Change the Enable Secret set during installation</li> <li>• Enable/Disable ssh access</li> <li>• Change ssh settings</li> </ul>
Data Export > Splunk Indexer	Configure a Splunk indexer
Data Export > Splunk Data	Configure the data to export to Splunk
Data Export > Syslog Servers	Configure Syslog servers.
Data Export > SysLog Data	Configure the data to export to Syslog servers.
Data Export > Reporting Database	Configure the authentication token for the Reporting Database and the data to export
Log Upload	Upload log files to an external server.
SNMP	Configure SNMP servers
Email Settings	Configure SMTP settings for communication between Ivanti EPMM and devices
Port Settings	Change default port configuration for Ivanti EPMM
Data Purge	Configure automated data purging
Services	Enable/Disable Ivanti EPMM services

## Network: Interfaces

Use the **Settings > Network > Interfaces** menu options to change parameters for the following network interface points for Ivanti EPMM:

- **Physical interfaces:** are configured as part of the installation process.
- **Virtual Local Area Network (VLAN) interfaces:** are optional interfaces you can configure on Ivanti EPMM to manage bandwidth and load balancing.

This section includes the following topics:

- ["Physical interface mapping to M2600 NIC ports" below](#)
- ["Changing physical interfaces" on the next page](#)
- ["Modify Interface window field description" on the next page](#)
- ["Adding VLAN interfaces" on the next page](#)
- ["Add VLAN window field description" on page 17](#)
- ["Deleting a VLAN interface" on page 17](#)

### Physical interface mapping to M2600 NIC ports

The following table provides a mapping of the physical interface name in the Ivanti EPMM System Manager to the physical NIC port in the M2600 appliance.

**TABLE 3.** PHYSICAL INTERFACE MAPPING TO M2600 NIC PORTS

Physical interface	M2600 NIC port
GigabitEthernet1	I - eth0 (NIC-3)
GigabitEthernet2	J - eth1 (NIC-4)
GigabitEthernet3	K- eth2 (NIC-5)
GigabitEthernet4	L- eth3 (NIC-6)
GigabitEthernet5	C- eth4 (NIC-1)
GigabitEthernet6	D- eth5 (NIC-2)

## Changing physical interfaces

### Procedure

To change a physical interface:

1. In the Ivanti EPMM System Manager, go to **Settings > Network > Interfaces**.
2. Click the interface name in the **Physical Interfaces** group to open the **Modify Interface** window.
3. Modify one or more of the interface fields, as necessary.

Refer to the "[Modify Interface window field description](#)" below table for details.

4. Click **Apply > OK** to save the changes.

## Modify Interface window field description

The following table summarizes fields and descriptions in the **Modify Interface** window:

**TABLE 4.** MODIFY INTERFACE WINDOW FIELD DESCRIPTION

Fields	Description
IP	Enter the IP address of the physical network interface.  Unless you are configuring a standalone implementation for a small trial, you should specify at least one physical interface.
Mask	Enter the netmask of the physical network interface.
ACL Name	Select an Access Control List for this interface.
Admin State	To enable this interface for use with the Ivanti system, click <b>Enable</b> . To temporarily prevent use of this interface with the Ivanti system, click <b>Disable</b> .

## Adding VLAN interfaces

The following describes how to add a VLAN interface.

### Procedure

1. In the Ivanti EPMM System Manager, go to **Settings > Network > Interfaces**.
2. Go to the VLAN Interfaces group.



3. Click **Add** to open the **Add VLAN** window.
4. Configure the VLAN interface, as necessary.  
Refer to the ["Add VLAN window field description" below](#) table for details.
5. Click **Apply** > **OK** to save the changes.

## Add VLAN window field description

The following table summarizes fields and descriptions in the **Add VLAN** window:

**TABLE 5.** VLAN WINDOW FIELD DESCRIPTION

Fields	Description
VLAN ID	Specify a number between 2 and 4094.
IP Address	Enter the IP address for this VLAN interface.
Mask	Enter the netmask for this VLAN interface.
Physical Interface	Select the physical interface that corresponds to this VLAN interface.
ACL Name	Select an Access Control List for this interface. See <a href="#">"Portal ACLs window" on page 74</a> .
Admin State	To enable this interface, click <b>Enable</b> . To temporarily suspend use of this VLAN, click <b>Disable</b> .

## Deleting a VLAN interface

The following describes how to delete a Virtual Local Area Network (VLAN) interface:

### Procedure

1. In the Ivanti EPMM System Manager, go to **Settings > Network > Interfaces**.
2. Go to the VLAN Interfaces group.
3. Select the VLAN you want to remove.
4. Click **Delete > Yes**.

## Network: Routes

Use the **Network > Routes** menu options to create and maintain static network routes within the enterprise. This section includes the following topics:

- ["Adding network routes " below](#)
- ["Add Route window" below](#)
- ["Deleting a network route" below](#)

### Adding network routes

#### Procedure

1. Log into System Manager.
2. Go to **Settings > Network > Routes**.
3. Click **Add** to open the **Add Route** window.
4. Configure the network route, as necessary.

Refer to the ["Add Route window" below](#) table for details.

5. Click **Apply > OK** to save the changes.

### Add Route window

The following table summarizes fields and descriptions in the **Add Route** window:

**TABLE 6.** ADD ROUTE WINDOW

Fields	Description
Network	Enter the network IP address.
Mask	Enter the subnet mask.
Gateway	Enter the IP address for the gateway.

### Deleting a network route

To delete a network route:

1. Log into System Manager.

2. Go to **Settings > Network > Routes**.
3. Select the entry you want to delete.
4. Click **Delete > Yes**.

## DNS and Hostname

Use the **Settings > DNS and Hostname** window to manage the hostname, default domain, and DNS information entered during installation. This section includes the following topics:

- ["Modifying the DNS configuration" below](#)
- ["DNS Configuration window" below](#)

## Modifying the DNS configuration

### Procedure

To modify the DNS configuration and hostname:

1. Log into System Manager.
2. Go to **Settings > DNS and Hostname** to display the **DSN Configuration** options.
3. Configure the host, as necessary. Refer to the ["DNS Configuration window" below](#) table for details.
4. Click **Apply > OK** to save the changes.

## DNS Configuration window

The following table summarizes fields and descriptions in the **DNS Configuration** window:

**TABLE 7.** DNS CONFIGURATION WINDOW

Fields	Description
Host name	Specify the fully-qualified host name for the appliance.
Default Domain	Specify the default domain for the appliance.
Preferred DNS Server	Specify the IP address of the primary DNS server to use.
Alternate DNS Server 1	Specify the IP address of an optional alternate DNS server.
Alternate DNS Server 2	Specify the IP address of an optional alternate DNS server.

## Static Hosts

Use the **Settings > Static Hosts** options to edit the hosts file when:

- DNS is not available or does not resolve the necessary names.
- DNS resolves the hostname to the external IP, but you want the traffic to go via the internal IP.

This section includes the following topics:

- ["Adding hosts" below](#)
- ["Add Host window" below](#)
- ["Editing hosts" on the next page](#)

## Adding hosts

### Procedure

1. Log into System Manager.
2. Go to **Settings > Static Hosts**.
3. Click **Add** to open the **Add Host** window.
4. Configure the host, as necessary. Refer to the ["Add Host window" below](#) table for details.
5. Click **Apply > OK** to save the changes.

## Add Host window

The following table summarizes fields and descriptions in the **Add Host** window:

**TABLE 8.** ADD HOST WINDOW

Fields	Description
IP Address	The IP address for the host you are adding.
FQDN	The fully-qualified domain name for this host, as in appdoc1.mycompany.com.
Alias	The alias for this host.

## Editing hosts

### Procedure

1. Log into System Manager.
2. Go to **Settings > Static Hosts**.
3. Click the IP address to open the **Modify Host** window.
4. Edit the fields, as necessary. Refer to the ["Add Host window" on the previous page](#) table for details.
5. Click **Apply > OK** to save the changes.

## Deleting hosts

### Procedure

1. Log into System Manager.
2. Go to **Settings > Static Hosts**.
3. Select the entry you want to delete.
4. Click **Delete > Yes**.

## Date and Time (NTP)

Use the **Settings > Date and Time (NTP)** options to manage Network Time Protocol (NTP) information specified during installation. This configuration step is optional, but is recommended due to the effect of database timestamps on the behavior of the system, as well as on the quality of reporting.

Currently, only UTC time format is supported for NTP. If you want to use a time format other than UTC, you must choose the local time source instead.

This section includes the following topics:

- ["Editing date and time" below](#)
- ["Data and Time window" on the next page](#)

## Editing date and time

### Procedure

1. Log into System Manager.
2. Go to **Settings > Date and Time (NTP)**.

3. Edit the fields, as necessary. Refer to the ["Data and Time window" below](#) table for details.
4. Click **Apply** > **OK** to save the changes.

## Data and Time window

The following table summarizes fields and descriptions in the **Date and Time** window:

**TABLE 9.** DATE AND TIME WINDOW

Fields	Description
Time Source	<ul style="list-style-type: none"><li>• Select <b>NTP</b> if you intend to specify one or more NTP servers.</li><li>• Select <b>Local</b> if you intend to use the system time of the Ivanti EPMM Server.</li></ul>
<b>If you select NTP for the time source</b>	
Primary Server	Specify the IP address or fully-qualified host name for the NTP server to use.
Secondary Server	Specify the IP address or fully-qualified host name for the first failover NTP server to use.
Tertiary Server	Specify the IP address or fully-qualified host name for the second failover NTP server to use.
<b>If you select Local for the time source</b>	
Date	Enter the current date.
Time (Hours:Mins:Secs)	Enter the current time in hours, minutes, and seconds.

## CLI

Use the **Settings** > **CLI** options to manage command line interface access settings specified during configuration. This section includes the following topics:

- ["Editing CLI settings" on the next page](#)
- ["CLI Configuration window " on the next page](#)

## Editing CLI settings

### Procedure

1. Log into System Manager.
2. Go to **Settings > CLI** to open the CLI Configuration window.
3. Modify one or more of the CLI fields, as necessary. Refer to the "[CLI Configuration window](#) " below table for details.
4. Click **Apply > OK** to save the changes.

## CLI Configuration window

The following table summarizes fields and descriptions in the **CLI Configuration** window:

**TABLE 10.** CLI CONFIGURATION WINDOW

Fields	Description
Enable Secret	Click the <b>Change Enable Secret</b> link to require users to enter a password in order to use the CLI.
Confirm Enable Secret	Re-enter the specified password to confirm. This field displays only if you click the <b>Change Enable Secret</b> link.
CLI Session Timeout (minutes)	Specify the duration of inactivity on the SSH connection that will cause the session to time out.
SSH	Select <b>Enable</b> if you want to allow SSH access to the Ivanti EPMM Administration tool.
Max SSH Sessions	Specify the maximum number of simultaneous SSH sessions to allow.

## Data Export: Splunk

The following system statistics are forwarded to the Splunk Indexer:

- **Ivanti EPMM server:** Java Virtual Machine (JVM)
- **CPU:** including an overview and breakdown by host, process, user, stat, and source.
- **Memory:** including an overview and breakdown by host, process, user, and source.
- **Disk:** including usage by host, source, and files opened by command, type, and user.
- **Network:** including interfaces, interface throughput, connection details, and network sources.

This section includes the general workflow to configure the Splunk Indexer:

<b>Step 1</b>	" <a href="#">Enabling the Splunk Forwarder</a> " <a href="#">below</a> to turn on the Splunk Forwarder so it can push data to the Splunk Indexer.
<b>Step 2</b>	" <a href="#">Adding a Splunk Indexer</a> " <a href="#">below</a> to configure which external Splunk Indexer will receive and manipulate the data from the Splunk Forwarder.
<b>Step 3</b>	" <a href="#">Configuring Splunk Data</a> " <a href="#">on the next page</a> to configure which data Splunk Forwarder sends to the Splunk Indexer.

## Enabling the Splunk Forwarder

### Procedure

1. Log into System Manager.
2. Go to **Settings > Services**.
3. Select **Enable** next to **Splunk Forwarder**.
4. Click **Apply > OK** to save the changes.

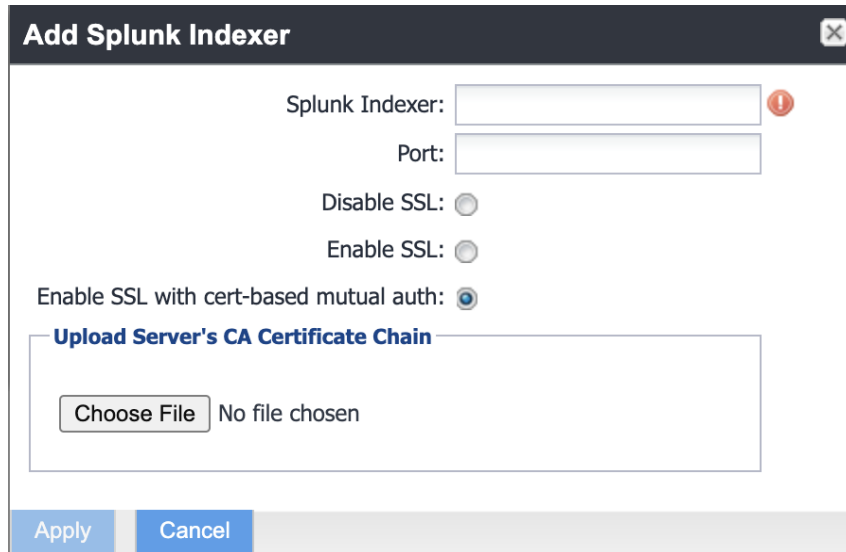
## Adding a Splunk Indexer

### Procedure

1. Log into System Manager.
2. Go to **Settings > Data Export > Splunk Indexer**.



- Click **Add** to open the **Add Splunk Indexer** window.



- Modify the fields, as necessary. See the following table for descriptions.

**TABLE 11.** ADD SPLUNK INDEXER WINDOW

Fields	Description
<b>Splunk Indexer</b>	Add the IP address of your Splunk Enterprise Server.
<b>Port</b>	Add the port number of your Splunk Enterprise Server.
<b>Disable SSL</b>	Click to disable Secure Socket Layer (SSL) encrypted communication.
<b>Enable SSL</b>	Click to enable or re-enable SSL encrypted communication.
<b>Enable SSL with cert-based mutual auth</b>	Click to enable or re-enable SSL with certificate-based mutual authentication. Select this option to connect to Splunk Heavy Forwarder for secure mutual authentication to Splunk.
<b>Choose file</b>	Click <b>Choose File</b> and browse to the CA certificate chain. Select it and click <b>OK</b> .

- Click **Apply** > **OK** to save the changes.

## Configuring Splunk Data

### Procedure

To configure the data to export to Splunk:

1. Log into System Manager.
2. Go to **Settings > Data Export > Splunk Data** to open the **Data to Index** window.
3. Modify the fields, as necessary. Click **Show/Hide Advanced Options** to further customize which data to send to Splunk.
4. Click **Apply > OK**.
5. Restart the Splunk Forwarder by disabling it, then enabling it again.
  - a. Go to **Settings > Services**.
  - b. Select **Disable** next to **Splunk Forwarder**.
  - c. Click **Apply > OK**.
  - d. Select **Enable** next to **Splunk Forwarder**.
6. Click **Apply > OK** to save the changes.

## Configuring Splunk certificates

### Procedure

Configure the Splunk client certificate in Ivanti System Manager at **Security > Certificate Mgmt > Splunk Client certificate**.

Configure the Splunk server certificate in Ivanti System Manager at **Data export> Splunk indexer page**.

## Data Export: SysLog

SysLog is a standard for message logging. You can use a syslog server to gather, analyze, and report on Ivanti EPMM activity. Using the System Manager, you configure the syslog servers that receive syslog data. You also can configure which data to export to which syslog server, and the format of the exported data.

Ivanti EPMM logs the following as Syslog events:

- Android client authentication failure events
- Failure to establish connection to determine revocation status
- Failure to establish TLS session
- Failure to generate key pair
- Key randomization failure
- Number of registered devices exceeded for this user

- Self test failure
- Self test start
- SSH connection failed
- Trusted channel during device enrollment
- X.509 certificate validation failure
- Certificate related events, including the following Certificate Expiry events:
  - Portal HTTPS Certificate
  - Client TLS Certificate
  - iOS Enrollment Certificate



Syslog events are stored on Ivanti EPMM and copied to the configured Syslog servers. The logs remain on Ivanti EPMM until deleted as part of the default log rotation process. View the data in System Manager at **TroubleShooting > Logs > View Module Logs**.

SysLog support on Ivanti EPMM includes:

- Secure connections between Ivanti EPMM and your syslog servers using TLS over TCP.
- Ability to specify which data to export, which allows you to:
  - Adhere to your security requirements.
  - Improve performance on both Ivanti EPMM and your syslog servers, as well as disk usage requirements on your syslog servers.
  - Focus only on data of interest to you.
- Ability to format the exported syslog data to meet your needs by using syslog templates.

## Exporting syslog data

This section includes the general workflow to export syslog data:

<b>Step 1</b>	" <a href="#">Configuring the syslog servers</a> " on the next page to receive the exported syslog data.
<b>Step 2</b>	" <a href="#">View Data Export: SysLog Advanced Options categories</a> " on page 30 to export to the syslog servers.

## Configuring the syslog servers

### Procedure

1. Log into System Manager.
2. Select **Settings > Data Export > SysLog Servers**.
3. Click **Add** to open the **Add SysLog** window.
4. Modify the fields, as necessary. Refer to the "Add SysLog window " below table for details.
5. Click **Apply > OK** to save the changes.

### Add SysLog window

The following table summarizes fields and descriptions in the **Add SysLog** window:

**TABLE 12.** FIELDS IN THE ADD SYSLOG WINDOW

Fields	Description
<b>Server</b>	Enter the host name for the remote syslog server.
<b>Protocol</b>	<p>Select the protocol to use between Ivanti EPMM and the syslog server.</p> <p>If you have more than one syslog server, you cannot use TCP on one of them and TLS over TCP on another. You can use UDP on one server and TCP or TLS over TCP on another.</p>
<b>Trusted Server Certificate</b>	<p>This field displays only if you select <b>TLS over TCP</b> for the <b>Protocol</b>.</p> <p>Upload a PEM-formatted file containing a valid issuing certificate authority (CA) certificate. When the syslog server presents its identity certificate to Ivanti EPMM, Ivanti EPMM validates the identity certificate to the CA certificate that you upload here.</p>
<b>Admin State</b>	Select <b>Enable</b> from the dropdown list if you want Ivanti EPMM to send syslog data to the configured syslog server. Select <b>Disable</b> to suspend use of the syslog server.
<b>Template</b>	<p>Enter a syslog template to format the logged messages.</p> <p>Example:</p> <pre>&lt;%pri%&gt;%protocol-version% %timestamp:::date-rfc3339% %HOSTNAME:% %app-name% %procid% %msgid% [TOKEN@11058 tag="RsyslogTLS"] %msg%</pre>
<b>Severity (facility.level)</b>	Enter *.* to send all messages to the syslog server for all syslog facilities and severity levels that Ivanti EPMM supports.

**TABLE 12.** FIELDS IN THE ADD SYSLOG WINDOW (CONT.)

Fields	Description
	<p>To filter which messages are sent to the syslog server, provide a syslog regular expression based on the form:</p> <p><b>&lt;facility keyword&gt; &lt;severity level keyword&gt;</b></p> <p>where:</p> <ul style="list-style-type: none"> <li>One of the following syslog facility keywords listed on <b>Settings &gt; Data Export &gt; SysLog Data</b>: <ul style="list-style-type: none"> <li><b>local3</b> - Virtual machine data (such as tomcat memory logs)</li> <li><b>local4</b> - Health data (such as Apache and Linux logs)</li> <li><b>local6</b> - Device data (such as Ivanti EPMM access from devices and Admin Portal)</li> <li><b>local7</b> - Audit data (Audit logs, which are also available on the Admin Portal at <b>Logs &gt; Audit Logs</b>)</li> </ul> </li> <li>The syslog severity level keyword, such as <b>info</b> and <b>warning</b>, specifies the minimum severity level to log.</li> </ul> <p><b>Example</b></p> <p><b>local6.*</b> - For all messages relating to device data</p> <p><b>local6.error</b> - For error messages relating to device data</p> <p><b>local6,local7.*</b> - For all messages relating to device data and audit logs</p> <p><b>*.*; local3,local7</b> - For all messages excluding those relating to virtual machine data and audit data.</p> <p><b>*.info</b> - For all messages with a severity of info or higher</p> <p><b>local4.warn</b> - For all messages relating to health data with a severity of warn or higher</p> <p><b>*.=debug</b> - For all messages with a severity of debug</p>



Syslog may experience data loss when logging messages especially when high volume of data is generated. For example, audit logs.

If you encounter performance issues with Syslog while exporting large amounts of data (like Audit logs), disable the export.

## View Data Export: SysLog Advanced Options categories

### Procedure

1. Log into System Manager.
2. Go to **Settings > Data Export > SysLog Data** to open the **Data to Index** window.
3. Click **Advanced Options** to display the categories within each set of data you want to modify.

## Configuring the syslog data to export

### Procedure

1. Log into System Manager.
2. Go to **Settings > Data Export > SysLog Data** to open the **Data to Index** window.
3. Click **Advanced Options** to display the categories within each set of data you want to modify.
4. Modify one or more of the fields, as necessary.
5. Change time intervals, as necessary. An interval indicates how often Ivanti EPMM collects the information and adds it to syslog data.
6. Click **Apply > OK** to save the changes.

## Data Export: Reporting Database

Monitor and reporting database (RDB) is a reporting database for Ivanti EPMM that provides a source you can query for creating reports. Use the **Settings > Data Export > Reporting Database** options to:

- ["Generating the authentication token" below](#)
- ["Configuring the Reporting Database Exporter" on the next page](#)

Refer to the *Monitor and Reporting Database Essentials* for information on configuring and using the Reporting Database.

## Generating the authentication token

### Procedure

To generate the authentication token for the Reporting Database:

1. Log into System Manager.
2. Go to **Settings > Data Export > Reporting Database**.

3. Go to the **Authentication Token** box.
4. Click **Generate**.
5. Copy the displayed token to the clipboard. Use this token in "[Configuring the Reporting Database Exporter](#)" below.

## Configuring the Reporting Database Exporter

### Procedure

To configure the Reporting Database Exporter:

1. Log into System Manager.
2. Select **Settings > Data Export > Reporting Database**.
3. Go to Export Configuration > **Data to Export**.
  - Check data categories to specify the data to export.
  - Clear data categories to specify the data to omit.

The **Device** option is required and cannot be cleared.

4. Select a frequency for **Run RDB Export Every**.
5. Select a retention time for **Retain Export Data For**.
6. Click **Apply > OK** to save the changes.

## SNMP

Ivanti EPMM provides (Simple Network Management Protocol (SNMP) capabilities. SNMP is a protocol used for network management for collecting information about network entities, such as servers and devices, on an Internet Protocol (IP) network. Various third-party SNMP systems are available that provide SNMP-based management and tools.

Ivanti EPMM provides the following SNMP capabilities:

- Ivanti EPMM sends these two SNMP traps (events) to a specified SNMP trap receiver using the SNMP v2c protocol.
- Link up and down traps

- An SNMP server can request information from Ivanti EPMM related to these management information bases (MIBs):
  - The HOST-RESOURCES-MIB
  - Apache web server configuration and status values (APACHE2-MIB).
  - disk I/O (UCD-DISKIO-MIB)
- Support for SNMP v2c and v3 protocols to pull MIB information from Ivanti EPMM to the SNMP server.



Ivanti EPMM limits Incoming SNMP requests to around 10 SNMP requests per minute.

## Configuring SNMP on Ivanti EPMM

This section includes the general workflow to configure SNMP:

<b>Step 1</b>	"Configuring the SNMP trap receiver server" below to which Ivanti EPMM sends SNMP traps.
<b>Step 2</b>	"Enabling the SNMP service with the v3 protocol" on the next page from whom Ivanti EPMM accepts requests.
<b>Step 3</b>	"Enabling the SNMP service with the v2c protocol" on page 35 between Ivanti EPMM and your SNMP server.

### Configuring the SNMP trap receiver server

Configure the server to which Ivanti EPMM sends SNMP traps. This server can also get MIB information from Ivanti EPMM.

#### Procedure

1. Log into System Manager.
2. Go to **Settings > SNMP** to open the SNMP details pane.
3. Click **Add** to open the **Add SNMP Trap Receiver** window.
4. Edit the fields, as necessary.

Refer to the "Add SNMP Trap Receiver window" below table for details.

5. Click **Apply > OK** to save the changes.



## Add SNMP Trap Receiver window

The following table summarizes fields and descriptions in the **Add SNMP Trap Receiver** window:

**TABLE 13.** ADD SNMP TRAP RECEIVER VALUES

Fields	Description
<b>Server</b>	Enter the server name for your SNMP trap receiver.  For example: <b>trapreceiver.myCompanyDomain.com</b>
<b>Port</b>	Enter the port number for your SNMP trap receiver.
<b>Community</b>	Enter the string which names the SNMP community on your SNMP trap receiver.
<b>Version</b>	Ivanti EPMM sends SNMP traps using SNMP protocol V2c. You can choose V2c or V3 for MIB requests.
<b>Admin State</b>	Select <b>Enable</b> to enable the SNMP service for this SNMP server.

## Deleting SNMP trap receiver servers

### Procedure

To delete one or more SNMP trap receiver servers:

1. Log into System Manager.
2. Go to **Settings > SNMP** to open the SNMP details pane.
3. Select one or more of the servers you want to delete.
4. Click the box next to **Server** to select all servers in the list.
5. Click **Delete > Yes**.

## Enabling the SNMP service with the v3 protocol

Set up the SNMP v3 user from whom Ivanti EPMM accepts requests. In addition, you can enable or disable sending traps to any configured SNMP trap receiver.

### Procedure

To enable the SNMP service with the SNMP v3 protocol:

1. Log into System Manager.
2. Go to **Settings > SNMP** to open the SNMP details pane.
3. Go to the **SNMP Control section > SNMP Service**.
4. Select **Enable** to enable the SNMP service on EPMM.
5. Go to the **Protocol** option and verify that **v3** is selected. The v3 option is selected, by default.
6. Click **Add** to open the **Add SNMP v3 User** window.
7. Enter the SNMP v3 user fields, as necessary. Refer to the ["Add SNMP v3 User window" below](#) for details.
8. Click **Save** to add this user to the **SNMP v3 Users** table.
9. Go to **Link Up/Down Trap**.
10. Click **Enable**. Select **Disable** to stop Ivanti EPMM from sending SNMP traps to any SNMP trap receiver.
11. Click **Apply > OK** to save the changes.

## Add SNMP v3 User window

**TABLE 14.** ADD SNMP v3 USER WINDOW

Fields	Description
User Name	Enter the user name without any spaces (example: miuser).
Security Level	Select a security level for authentication. The options are: <ul style="list-style-type: none"> <li>• <b>noAuthNoPriv</b>: Without Authentication or Privacy.</li> <li>• <b>authNoPriv</b>: With Authentication and without Privacy</li> <li>• <b>authPriv</b>: With Authentication and Privacy</li> </ul>
Auth Protocol	Select an authentication protocol. This can be selected only if the <b>Security Level</b> is selected as <b>authNoPriv</b> or <b>authPriv</b> .
Auth Password	Enter the Auth Password with a minimum of 8 characters.  Note: From 11.12.0.0 release, the Auth password will not support these characters: '\$', '"', '\', ' ', '`'. Also, existing passwords that contain these characters must be updated before saving SNMP settings.
Privacy Protocol	Select a privacy protocol. This can be selected only if <b>Security Level</b> is selected as <b>authPriv</b> .
Privacy Password	Enter a privacy password with minimum of 8 characters.

**TABLE 14.** ADD SNMP v3 USER WINDOW (CONT.)

Fields	Description
	Note: From 11.12.0.0 release, the Privacy password will not support these characters: '\$', ';', '"', '\', '' Also, existing passwords that contain these characters must be updated before saving SNMP settings.

## Deleting SNMP v3 users

### Procedure

1. Log into System Manager.
2. Go to **Settings > SNMP** to open the SNMP details pane.
3. Go to the **SNMP Control** group.
4. Select one or more of the users you want to delete. Click the box next to **User Name** to select all users in the list.
5. Click **Delete > Yes**.

## Enabling the SNMP service with the v2c protocol

Set up the SNMP v2c communication between Ivanti EPMM and your SNMP server. You also enable or disable sending traps to any configured SNMP trap receiver.

### Procedure

1. Log into System Manager.
2. Go to **Settings > SNMP** to open the SNMP details pane.
3. Go to the **SNMP Control section > SNMP Service**.
4. Select **Enable** to enable the SNMP service on EPMM.
5. Go to the **Protocol** option and select **v2**.
6. Change the value of **Read Only Community** if necessary. The standard SNMP community name is **public**. This is the community the SNMP server uses to pull MIB information from EPMM.
7. Go to the **Link Up/Down Trap** option and select **Enable**. Select **Disable** to stop Ivanti EPMM from sending SNMP traps to any SNMP trap receiver.
8. Click **Apply > OK** to save the changes.

## Log Upload

Use the **Settings > Log Upload** options to upload Ivanti EPMM log files to an external server when you are working with Ivanti Technical support or an Ivanti partner to troubleshoot an issue in Ivanti EPMM. You can upload the following files:

- Log files (see ["Exporting logs" on page 145](#) in the Troubleshooting chapter for more information)
- System monitor files (see ["System monitor" on page 148](#) in the Troubleshooting chapter for more information)

### Setting a log upload user

#### Procedure

1. Log into System Manager.
2. Go to **Settings > Log Upload** to open the **Log Upload** details page.
3. Fill out the fields in one of the following server groups:
  - SFTP Server Configuration
  - HTTPS Server Configuration
4. Typically, you will use the default HTTPS Server Configuration, which automatically includes the user name you entered in **Maintenance > Software Updates**. Confirm with Ivanti Technical Support that the entries on this display are correct.
5. Click **Apply > OK** to save the changes.

## Email Settings

Use the **Settings > Email Settings** options to set up SMTP server access required for Ivanti EPMM email alerts, such as policy violation alerts.

In the US and certain other countries, the SMTP server settings are also required for alerts sent via SMS. In a few cases, the SMTP server might be used to transmit a control command to certain devices.

This section includes the following topics:

- ["Testing email configurations" below](#)
- ["Testing email configurations" below](#)

- ["Deleting the email configuration" below](#)

## Testing email configurations

### Procedure

To test your email configuration:

1. Log into System Manager.
2. Go to **Settings > Email Setting** to open the **Email Configuration** window.
3. Edit the fields, as necessary. Refer to the ["Deleting the email configuration" below](#) table for details.
4. Click the **Test** button to open the **Test Email** window.
5. Enter an email address and body for the test email.
6. Click **Send**.
7. Confirm that the email arrived.
8. Click **Apply > OK** to save the changes.

## Deleting the email configuration

You can delete the email configuration. When deleted, Ivanti EPMM can no longer send email alerts, such as policy violation alerts, to devices.

### Procedure

To delete the email configuration:

1. Log into System Manager.
2. Go to **Settings > Email Setting** to open the **Email Configuration** window.
3. Click **Delete**.
4. Click **Yes** to proceed.

## Email Configuration window

The following table summarizes fields and descriptions in the **Email Configuration** window:

**TABLE 15.** FIELDS AND DESCRIPTIONS IN THE EMAIL CONFIGURATION WINDOW

Fields	Description
From Email	<p>Specify the email address to use in the From field for all administrative email notifications.</p> <p>Make sure that the account for this email address has the right privileges to send emails to internal and external email domains.</p>
SMTP Server	Specify the IP address or fully-qualified host name for the SMTP server the server will use.
SMTP Server Port	Specify the port configured for the SMTP server.
Protocol	If the SMTP server you are configuring is a secured server, that is, it uses the SMTPS protocol, then select the <b>SMTPS</b> button. Otherwise, leave <b>SMTP</b> selected. If you want to allow an existing connection to upgrade to an encrypted connection, select <b>SMTP with STARTTLS</b> .
Authentication Required	Specify whether this SMTP server requires authentication. In most cases, this field will be set to <b>Yes</b> .
User Name	If you select <b>Yes</b> for <b>Authentication Required</b> , then this field displays. Enter the user name required for SMTP authentication.
Password	If you select <b>Yes</b> for <b>Authentication Required</b> , then this field displays. Enter the password required for SMTP authentication.
Confirm Password	If you select <b>Yes</b> for <b>Authentication Required</b> , then this field displays. Confirm the password required for SMTP authentication.

## Port Settings

Use the **Settings > Port Settings > Port Configuration** options to change settings for the following Ivanti services:

- Sync TLS
- MIFS Admin
- Sentry Service
- Apps@Work
- Local CA Certificate Revocation List

## Port setting considerations

- If you enable client mutual certificate authentication, you must change the **Apps@Work Port** setting if you are using iOS devices with the Apps@Work web clip using certificate authentication.
- Other changes to the default port settings are seldom necessary.
- Making changes to these settings sometimes requires that you re-register devices, so use caution when making changes.

## Changing port settings

### Procedure

1. Log into System Manager.
2. Go to **Settings > Port Setting** to open the **Port Configuration** window.
3. Edit the fields, as necessary.
4. Refer to the "[Port Configuration window](#)" on the next page table for details.



---

The port and protocol default values for newly-issued Local CA Certificate Revocation List (CRL) distribution points (CDP) have changed. Beginning with the 10.4 Ivanti EPMM release, new Local CDPs will use port 8080 and protocol HTTP by default. You don't need to generate a new CSR or replace the old certificates. Local CDPs that were configured to use HTTPS through port 443 will still be reachable.

---

## Changing the default CRL protocol and port configuration

Use the **Settings > Port Settings > CRL (Certificate Revocation List) protocol and port configuration** options to change the default protocol and port for all local certificate authorities (CA).



---

For new installations, the default value for the certification revocation list (CRL) is protocol HTTP and port 8080. The need to change the default port is rare. However, if you do modify the CRL port, verify that no other Ivanti EPMM service is using that port. For example, port 9997 is the default value for Sync TLS, and using the same port for CRL will result in service disruptions.

---

### Procedure

1. Log into System Manager.
2. Go to **Settings > Port Settings** to open the **Port Configuration** window.
3. Scroll down to the CRL (Certificate Revocation List) protocol and port configuration section.
4. Select the default CRL protocol.
  - CRL Protocol: **HTTPS** or **HTTP**
  - CRL Port: defaults to the port supporting the selected protocol. If you choose HTTP, you can leave the default (8080), or modify the CRL port number.



When the CRL port and protocol changes, verify that the old port is open on the network firewall. Otherwise, Apps (such as Apps@Work) using certificates from before the port change will timeout during the certificate revocation verification check.

---

5. Click **Apply**.
6. Click **Save** (in the top-right of the page) to globally save your choices when the system is rebooted.

## Verifying Sentry connectivity

### Procedure

To verify that Standalone Sentry is successfully connecting with Ivanti EPMM:

1. Log into System Manager for the Standalone Sentry.
2. Go to **Troubleshooting > Service Diagnosis**.
3. For **EMM** service, click **Verify**.
4. The Status for the **EMM** service should show **Success**.

## Port Configuration window

The following table summarizes fields and descriptions in the **Port Configuration** window:

Ivanti recommends to allow HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for EPMM server management and must have strictly controlled access.



**TABLE 16.** FIELDS AND DESCRIPTIONS OF THE PORT CONFIGURATION WINDOW

Fields	Description
Sync TLS Port	<p>Enter the port. However, changing this port from the default port 9997 is rare. This port cannot be the same as any other ports specified in the <b>Port Configuration</b> section.</p> <p>This port is used for Mobile@Work for iOS and Android registration and device check-ins and AppConnect check-ins when mutual authentication is not enabled.</p> <p>Select <b>Disable</b> to close this port <b>only if all</b> of the following are true:</p> <ul style="list-style-type: none"> <li>• This Ivanti EPMM is a new installation, not an upgrade.</li> <li>• You enable mutual authentication before any devices register.</li> <li>• iOS devices are using only Mobile@Work 9.8 for iOS through the most recently released version as supported by Ivanti.</li> </ul> <p>For more information, see "Mutual authentication between devices and Ivanti EPMM" in the <i>Ivanti EPMM Device Management Guide</i>.</p>
MIFS Admin Port	<p>You can change the MIFS Admin port from port 443 (the default) to port 8443. Using port 443 enhances the security of communications across the port because port 8443 can be blocked.</p>
Sentry Service Port	<p>The <b>Standalone Sentry is called the Sentry service port. Standalone Sentry communicates with Ivanti EPMM over port 8443 to get device information. The default Sentry service port is port 8443.</b></p> <p>Using port 8443 as the Sentry service port adds an additional layer of security. Typically, port 8443 is not accessible on the public Internet. Using port 8443 helps ensure that the Sentry service port is protected against unauthorized external access.</p> <p>Ivanti recommends that port 8443 is used as the Sentry service port. If your firewall rules do not allow connections to the Sentry service port on 8443, you can configure 443 as the Sentry service port.</p>

**TABLE 16.** FIELDS AND DESCRIPTIONS OF THE PORT CONFIGURATION WINDOW (CONT.)

Fields	Description
	<p>If the Sentry service port is 8443, Ivanti EPMM will only respond to requests on port 8443. Requests to 443 will be redirected to 8443. If the Sentry service port is 443, Ivanti EPMM will only respond to requests on port 443. Requests to 8443 will be redirected to 443.</p> <p>If the Sentry service port is 443, it is important that you define a Portal ACL for the Sentry connection.</p>
Apps@Work Port	<p>This port is used by Apps@Work on iOS, Android, and macOS devices to communicate with Ivanti EPMM. By default, it is port 443.</p> <p>Change the port in these cases:</p> <ul style="list-style-type: none"> <li>• If <b>both</b> of the following are true: <ul style="list-style-type: none"> <li>◦ You enabled client mutual certification authentication on the Admin Portal at <b>Settings &gt; Security &gt; Certificate Authentication</b>.</li> <li>◦ You are using iOS devices with the Apps@Work web clip using certificate authentication.</li> </ul> </li> <li>• If identity certificates with the root CA "CN=DigiCert Assured ID Root CA" are issued to iOS devices.</li> </ul> <p>For example, you might use identity certificates with this root CA in the Exchange, VPN, or Wi-Fi settings that you apply to iOS devices.</p> <p>If you change the port, Ivanti recommends port 7443. However, you can use any port except the port that the <b>MIFS Admin Port</b> uses, which is either 443 or 8443.</p>
Atlas Port	<p>Atlas is a legacy product of Ivanti EPMM versions prior to Ivanti EPMM 10.2.0.0. This feature is an Ivanti service which aggregates data from multiple Ivanti EPMMs, extending reporting and management services.</p> <p>The port is 443 by default, but you have the option to change it when enabled.</p>

Other port services not configurable from the UI include:

- **Sync service port** – Default port is 9999 and cannot be changed.
- **Provisioning protocol** – Default protocol is HTTPS and cannot be changed.
- **Provisioning port** – Default port is 443 cannot be changed

## Data Purge

Ivanti EPMM stores significant amounts of data in its database and log files. Every four hours, Ivanti EPMM automatically purges client logs and notification tables. You can automatically or manually purge other data. Purging enables you to:

- Manage system storage
- Fulfill corporate or legal requirements for data disposal

For example, a production system managing thousands of phones can exhaust available system storage. In addition, certain industries and countries must adhere to legal mandates requiring purging of data after a pre-defined period of time.

Ivanti EPMM provides a data purging feature that enables you to:

- turn auto-purging on/off
- configure auto-purging based on system storage usage or the age of the data
- manually purge audit log data
- manually purge old database data using CLI commands

This section includes the following topics:

- ["Configuring manual or automatic data purge" below](#)
- ["Configuring audit log purge" on the next page](#)
- ["Manually purging DB data using CLI commands" on page 45](#)
- ["Setting up the system storage alert" on page 45](#)

## Configuring manual or automatic data purge

You can configure auto-purging based on either the amount of system storage used or the age of the data stored. The page also displays the amount of data currently in system storage, and the last Ivanti EPMM run status for data and log files.

### Procedure

To configure purge values:

1. Log into the System Manager.
2. Go to **Settings > Data Purge**.
3. Set **Auto Purge** to **ON** or **Off**.
4. To purge data based on the age of the data:
  - Enter a value for **Keep data no more than \_\_ days**. The default is 90 days.
  - Enter a value for **Keep logs no more than \_\_ days**. The default is 30 days.

Selected times are based on the Ivanti EPMM system time.

5. Enter a time in the **Purge daily** drop-down menu to purge data and logs at a specific time each day. The default is 3 AM.
6. Purge data using one of the following options:
  - **Manual**: click **Apply** to configure settings then click **Purge Now** to begin manual purging.
  - **Automatic**: set the **Auto Purge** to **On**, configure settings, click **Apply> OK**.

## Configuring audit log purge

You specify how long audit logs are retained on Ivanti EPMM. Determining how long to retain data is a balance between having data you need and having the available server resources to run your Ivanti EPMM. The default value is 90 days.

### Procedure

To set how long audit logs are kept:

1. Log into the System Manager.
2. Go to **Settings > Data Purge > Audit Logs Purge Configuration**.

3. Select the number of days Ivanti EPMM retains log information. Select from the following options:
  - Last three months (the default)
  - Last one month
  - Last two months
  - Last three months
  - Last four months
  - Last six months
  - Last twelve months
4. Click **Apply** > **OK** to save the changes.

## Manually purging DB data using CLI commands

### Procedure

To use CLI commands to clean up the disk storage:

1. Use **ssh** to log in to Ivanti EPMM.
2. Enter **enable** to access EXEC PRIVILEGED CLI mode.
3. Enter the "enable secret" password.
4. Enter **dbcleanup purge\_data** to clean up the database. If Ivanti EPMM services are not already stopped, this command stops them and restarts them when it finishes the clean up.
5. Enter **diskcleanup retired\_devices** to clean up retired devices from the disk.
6. If Ivanti EPMM services were stopped, restart Ivanti EPMM.

## Setting up the system storage alert

You can set up a System Event to alert you when system storage reaches the level specified. You can use this alert, for example, to indicate the need for manual purging or to prompt personnel to confirm successful auto-purging.

### Procedure

To set up the system storage alert:

1. Log onto the Admin Portal.
2. Click **Logs** > **Event Settings**.

3. Click **Add New > System Event**.
4. Select **System storage threshold has been reached**.

## Services

Use the **Settings > Services** options to enable or disable the following Ivanti services:

- **Ivanti EPMM**: Ivanti EPMM service.
- **Splunk Forwarder**: Splunk Forwarder service.
- **Reporting Database Exporter**: Ivanti RDB (Reporting Database). Enabling the Reporting Database Exporter allows the Reporting Database to extract the relevant Ivanti EPMM data.
  - **Migrator**: Enabling this service is part of the procedures for migrating from Ivanti EPMM to Ivanti Neurons for MDM. It retrieves device information from Ivanti EPMM. Enable this service only if Ivanti Professional Services instructs you to.

## Managing Services

### Procedure

To manage these services:

1. Log into the System Manager.
2. Go to **Settings > Services**.
3. Select **Enable** or **Disable** next to any of the services.
4. Click the link to open a window to any running service.
  - You might need to log into the service.
  - The **Running** link for **Splunk Forwarder** is not a live link to the service. When you disable the Splunk Forwarder service, you also disable the connection to the Splunk indexers configured in **Settings > Data Export > Splunk Indexer**.
  - If you re-enable the Splunk Forwarder service, Ivanti EPMM re-connects to the indexers configured in **Settings > Data Export > Splunk Indexer**.
5. Click **Apply > OK** to save the changes.

# Security Settings

- [Identity Source: Password Policy](#)
- [Certificate Mgmt](#)
- [Access Control Lists: Network Services](#)
- [Access Control Lists: ACLs](#)
- [Access Control Lists: Portal ACLs](#)
- [Advanced: Host Header Validation](#)
- [Advanced: HSTS](#)
- [Advanced: Incoming SSL Configuration](#)
- [Advanced: Outgoing SSL Configuration](#)
- [Advanced: ModSecurity](#)
- [Advanced: SAML](#)
- [Advanced: Trusted Front End](#)
- [Advanced: Portal Authentication](#)
- [Advanced: SSH Configuration](#)

## Identity Source: Password Policy

Use the **Security > Identity Source > Password Policy** menu items to configure complex password requirements for local users. This section includes the following topics:

- ["System Manager local user password policy overview" below](#)
- ["Setting password policy" on page 49](#)
- ["Local user password complexity enforcement details" on page 50](#)
- ["Local user password strength enforcement details" on page 52](#)

## System Manager local user password policy overview

You can specify the password policy for System Manager local users.

The password policy includes the following:

- Enforcement type, which is one of the following:
  - ["Local user password complexity enforcement" below](#)
  - ["Local user password strength enforcement" on the next page](#)
- Ivanti EPMM enforces the password complexity or strength when:
  - You add a new local user in the System Manager.
  - Local users change their password.
- Number of failed attempts

After the local user fails to enter the correct password after the specified number of attempts, Ivanti EPMM does not allow the user to login until the specified auto-lock time has expired.

- Password history enforcement

When you enforce password history, local users **cannot** use the previous 4 passwords when changing their password.

## Local user password complexity enforcement

You can enforce password complexity requirements on local user passwords. Complex requirements prevent local users from using passwords that are weak and therefore easy to guess. However, requirements that are too complex make using the user ID and password inconvenient for the user because they have to enter a more complicated or longer password. Therefore, when you choose the complexity requirements, consider both your security needs and you local user convenience.

You specify the following password complexity requirements:

- Minimum and maximum password length
- Minimum number of character classes in a password

Character classes are:

- Lower case alphabetic characters
- Upper case alphabetic characters
- Numeric characters 0 through 9
- Special characters, which are `! = ( { [ _ : - ; ~ , ) } ] @ # ^ | $`

In addition to the requirements that you specify, Ivanti EPMM enforces the following requirements:



- The password cannot have a Grave accent (back tick) character.
- The password cannot contain the space character.
- The password cannot have 4 or more repeating characters.
- The password cannot be the same as the user ID.

**Related topics**

- ["Setting password policy" below](#)
- ["Local user password strength enforcement details" on page 52](#)

**Local user password strength enforcement**

You can specify the local user password strength to enforce how strong a password must be. Setting the password strength prevents local users from using passwords that are weak and therefore easy to guess. However, setting the password strength too high makes using the user ID and password inconvenient for the user because they have to enter a more complicated or longer password. Therefore, when you choose the password strength requirement, consider both your security needs and your local user convenience.

In addition to your specified password strength, the System Manager enforces the following requirements:

- The password cannot have a Grave accent (back tick) character.
- The password cannot contain the space character.
- The password length must be 128 or less.
- The password cannot be the same as the user ID.

**Related topics**

- ["Setting password policy" below](#)
- ["Local user password strength enforcement details" on page 52](#)

**Setting password policy****Procedure**

To set the password policy for System Manager local users:

1. Log into System Manager.
2. Select **Security > Identity Source > Password Policy**.

3. Select one of these options:

- **Enable Password Complexity Enforcement**

Modify one or more of the default fields, as necessary. See "[System Manager local user password policy overview](#)" on page 47.

- **Enable Password Strength Enforcement**

Modify one or more of the default fields, as necessary. See "[Local user password strength enforcement details](#)" on page 52.

4. Click **Apply > Yes > OK**.

5. Click **Reset to Default** followed by **OK** to reset the password policy to the default values.



Changing the password policy or resetting to default values can result in local users being disconnected or cause a disruption in service.

## Local user password complexity enforcement details

The following table summarizes the fields of the System Manager local user password policy when using password complexity enforcement:

**TABLE 17.** SYSTEM MANAGER LOCAL USER PASSWORD COMPLEXITY ENFORCEMENT FIELDS

Field	Description	Default value
<b>Enable Password Complexity Enforcement</b>	Select this field when you want to apply password complexity requirements to local user passwords.	Selected
<b>Minimum number of character classes in password</b>	<p>This field is only available when you selected <b>Enable Password Complexity Enforcement</b>.</p> <p>Select the minimum number of different character classes (lower case, upper case, numeric, and special character) that you require in a password.</p> <p>For each character class, you select whether it counts towards the minimum number. The minimum number must be less than or equal to the number of character classes you select.</p>	3

**TABLE 17.** SYSTEM MANAGER LOCAL USER PASSWORD COMPLEXITY ENFORCEMENT FIELDS (CONT.)

Field	Description	Default value
	For example, if the minimum number of character classes is 2, you can select 2 or more of the character classes. In this case, if you select <b>Lower Case</b> , <b>Upper Case</b> , and <b>Numeric</b> , the password must contain at least 2 of those character classes.	
<b>Lower Case</b>	Select this option if the lower case character class counts towards the minimum number of character classes that you require in a password.  The lower case character class includes the lower case alphabetic characters 'a' through 'z'.	Selected
<b>Upper Case</b>	Select this option if the upper case character class counts towards the minimum number of character classes that you require in a password.  The lower case character class includes the upper case alphabetic characters 'A' through 'Z'.	Selected
<b>Numeric</b>	Select this option if the numeric character class counts towards the minimum number of character classes that you require in a password.  The numeric character class includes the characters '0' through '9'.	Selected
<b>Special Character</b>	Select this option if the special character class counts towards the minimum number of character classes that you require in a password.  The special character class includes these characters:  != ( { [ _ : - ; ~ , ) } ] @ # ^   \$	Not selected
<b>Min Password Length</b>	Select the minimum number of characters in a password. Valid values are 6 through 16.	8
<b>Max Password Length</b>	Select the maximum number of characters in a password. Valid values are 21 through 128.	32

**TABLE 17.** SYSTEM MANAGER LOCAL USER PASSWORD COMPLEXITY ENFORCEMENT FIELDS (CONT.)

Field	Description	Default value
<b>Number of Failed attempts</b>	<p>Specify the number of failed attempts that a local user can make when entering his password.</p> <p>After this number of attempts, Ivanti EPMM does not allow the user to login until the specified auto-lock time has expired. After the auto-lock time expires, each failed login attempt results in Ivanti EPMM not allowing the user to login until the auto-lock time expires again.</p> <p>Valid values are 1 through 16.</p>	5
<b>Auto-Lock Time</b>	<p>Specify how much time in seconds the local user must wait before he can log in after exceeding the number of failed attempts.</p> <p>Valid values are 0 through 3600 seconds.</p>	30
<b>Enforce Passcode History (Last 4 passwords)</b>	<p>Select <b>Enable</b> if you do not want to allow a local user to use the previous 4 passwords when changing his password.</p> <p>To allow a local user to use the previous 4 passwords, select <b>Disable</b>.</p>	Enable

**Related topics**

- ["System Manager local user password policy overview" on page 47](#)
- ["Setting password policy" on page 49](#)

**Local user password strength enforcement details**

The following table summarizes the fields of the System Manager local user password policy when using password strength enforcement:

**TABLE 18.** SYSTEM MANAGER LOCAL USER PASSWORD STRENGTH ENFORCEMENT FIELDS

Field	Description	Default value
<b>Enable Password Strength Enforcement</b>	Select this field when you want to apply password strength requirements to local user passwords.	Not selected
<b>Number of Failed attempts</b>	<p>Specify the number of failed attempts that a local user can make when entering his password.</p> <p>After this number of attempts, Ivanti EPMM does not allow the user to login until the specified auto-lock time has expired. After the auto-lock time expires, each failed login attempt results in Ivanti EPMM not allowing the user to login until the auto-lock time expires again.</p> <p>Valid values are 1 through 16.</p>	5
<b>Auto-Lock Time</b>	<p>Specify how much time in seconds the local user must wait before he can log in after exceeding the number of failed attempts.</p> <p>Valid values are 0 through 3600 seconds.</p>	30
<b>Enforce Passcode History (Last 4 passwords)</b>	<p>Select <b>Enable</b> if you do not want to allow a local user to use the previous 4 passwords when changing his password.</p> <p>To allow a local user to use the previous 4 passwords, select <b>Disable</b>.</p>	Enable
<b>Password Strength</b>	<p>Select a value between 0 and 100, where 0 is the weakest requirement, and 100 is the strongest requirement.</p> <p>You can enter a value or move the slider.</p> <p>For details, see <a href="#">"Local user password strength value descriptions" on the next page.</a></p>	35

**Related topics**

- ["System Manager local user password policy overview" on page 47](#)
- ["Setting password policy" on page 49](#)

## Local user password strength value descriptions

The following table describes the System Manager local user password strength values:

**TABLE 19.** SYSTEM MANAGER LOCAL USER PASSWORD STRENGTH VALUE DESCRIPTIONS

Strength value	Description	Examples
0 - 20	<b>Weak: risky password</b>	<ul style="list-style-type: none"> <li>Few characters: <b>zxcvbn</b></li> <li>Sequences: <b>abcdefghijk987654321</b></li> <li>Names: <b>briansmith4mayor</b></li> <li>Words: <b>viking</b></li> <li>Words with number substitutions: <b>ScoRpi0ns</b></li> </ul>
21 - 40	<b>Fair: protection from throttled online attacks</b> <p>Throttled online attacks are attacks to guess the passcode which are:</p> <ul style="list-style-type: none"> <li>on the device</li> <li>rate-limited</li> </ul> <p>Rate-limited attacks are limited to some number of attempts per time period.</p>	<ul style="list-style-type: none"> <li>Few characters but with special characters: <b>qwER43@!</b></li> <li>Words plus numbers: <b>temppass22</b></li> <li>Names plus numbers: <b>ryanhunter2000</b></li> <li>Words with special character and number substitutions: <b>R0\$38uD99</b></li> <li>Names with capitalization: <b>verlineVANDERMARK</b></li> </ul>
41 - 60	<b>Good: protection from unthrottled online attacks</b> <p>Unthrottled online attacks are attacks to guess the passcode which are:</p> <ul style="list-style-type: none"> <li>on the device</li> <li>not rate-limited</li> </ul>	<ul style="list-style-type: none"> <li>Longer words with special character and number substitutions: <b>Tr0ub4dour&amp;3</b></li> <li>Longer phrases with numbers and special characters: <b>neverforget13/3/1997</b></li> <li>Longer letter, number, and special character combinations: <b>asdfghju7654rewq</b> <b>OEUIDHG&amp;*( )LS_</b></li> </ul>
61 - 80	<b>Strong: moderate protection from offline slow-hash scenario</b>	<ul style="list-style-type: none"> <li>Longer random letters and numbers: <b>zevusqr3</b> <b>esqu3Wil</b> <b>tgbvdnjuk</b></li> </ul>

**TABLE 19.** SYSTEM MANAGER LOCAL USER PASSWORD STRENGTH VALUE DESCRIPTIONS (CONT.)

Strength value	Description	Examples
	An offline slow-hash scenario is a sophisticated algorithm for guessing a passcode. The algorithm runs offline from the device after copying passcode-related files from the device.	<ul style="list-style-type: none"> <li>Longer phrases with numbers and special characters: <b>Compl3xChar\$</b></li> </ul>
81 - 100	<b>Very strong: strong protection from offline slow-hash scenario</b>	<ul style="list-style-type: none"> <li>Very long random characters: <b>eheuczkqyq</b> <b>rWibMFACxAUGZmxhVncy</b> <b>Ba9ZyWABu99</b> <b>[BK#6MBgbH88Tofv)vs\$w</b></li> <li>Long phrases: <b>correcthorsebatterystaple</b></li> <li>Long phrases with substitutions: <b>coRrecth0rseba+ +ery9.23.2007staple\$</b></li> </ul>

**Related topics**

- ["System Manager local user password policy overview" on page 47](#)
- ["Setting password policy" on page 49](#)

**Security overview**

System Manager **Security** menu options contains menu items for configuring Ivanti EPMU access. The following table summarizes the tasks associated with each menu item.

**TABLE 20.** SECURITY MENU ITEMS

Settings Menu	Task
Identity Source > Local Users	Create, delete, and manage local users for System Manager.
Identity Source > Password Policy	Set the password requirements for System Manager local users.
Certificate Mgmt	View and manage certificates for:

**TABLE 20.** SECURITY MENU ITEMS (CONT.)

Settings Menu	Task
	<ul style="list-style-type: none"> <li>• Portal HTTPS</li> <li>• Client TLS</li> <li>• iOS Enrollment</li> </ul>
Access Control Lists > Networks & Hosts	Create and manage entries for networks and hosts
Access Control Lists > Network Services	Create and manage entries for network services
Access Control Lists > ACLs	Compile access control lists
Access Control Lists > Portal ACLs	Compile access control lists for specific Ivanti EPMM components
Advanced settings - Most configurations do not require changing the following settings.	
Advanced > Host Header Validation	Enhances the security of HTTP traffic
Advanced > HSTS	Configure HTTP Strict Transport Security
Advanced > Incoming SSL Configuration	Select protocols and cipher suites other than the defaults for incoming SSL/TLS connections
Advanced > ModSecurity	Configure protection against certain types of future public security vulnerabilities
Advanced > Outgoing SSL Configuration	Select protocols and cipher suites other than the defaults for outgoing SSL/TLS connections.
Advanced > Outgoing SSL Configuration	Select protocols and cipher suites other than the defaults for outgoing SSL/TLS connections.
Advanced > SAML	Allow local administrator users to use single-sign on for the Admin Portal and self-service user portal. This feature also allows administrators to automatically redirect authentication for the Admin Portal and the user portal to your external Identity Provider (IdP).
Advanced > Trusted Front End	Configure a Trusted Front End between devices and Ivanti EPMM.



**TABLE 20.** SECURITY MENU ITEMS (CONT.)

Settings Menu	Task
Advanced > Admin/Self-Service User Portal Authentication	Select whether device users authenticate to the user portal, and whether administrators authenticate to the Admin Portal, with a password, a certificate, or either.
Advanced > SSH Configuration	Configure SSH to enable Public Key Authentication and Password Authentication.

## Identity Source: Local Users

System Manager maintains a user database that is separate from the Admin Portal database. The user you specify when you install Ivanti EPMM is created as a separate user in each database. All users in the System Manager database are local users with the following privileges that cannot be changed:

- Command Line Interface (CLI)
- System Manager access



**Important!** Local users in the System Manager database are separate users from the local users that you define in the Admin Portal.

Use the **Security > Identity Source > Local Users** menu options to perform the following tasks using:

- "Adding local System Manager users" below
- "Editing local System Manager users" on page 59
- "Deleting local System Manager users" on page 59

## Adding local System Manager users

### Procedure

To add a local user to the System Manager database:

1. Log into System Manager.
2. Go to **Security > Identity Source > Local Users**.
3. Click the **Add** button to open the **Add New User** window.

4. Modify one or more of the fields, as necessary.

Refer to ["Add New User window" below](#) table for details.

5. Click **Apply > OK**.

## Add New User window

The following table summarizes fields and descriptions in the **Add New Users** window:

**TABLE 21.** ADD NEW USER FIELDS

Fields	Description
User ID	Enter the unique identifier to assign to this user. The user ID is case sensitive.
First Name	Enter the user's first name.
Last Name	Enter the user's last name.
Password	<p>Enter a password for the user.</p> <p>Valid passwords are determined by the password policy for System Manager local users.</p> <p>For details, see:</p> <ul style="list-style-type: none"><li>• <a href="#">"System Manager local user password policy overview" on page 47</a></li><li>• <a href="#">"Setting password policy" on page 49</a></li></ul> <p>Enter a password for the user based on the Password Policy configured by the administrator in the System Manager (<b>Security &gt; Identity Source &gt; Password Policy</b>). However the following password requirements cannot be changed:</p> <ul style="list-style-type: none"><li>• cannot be the same as the user ID</li><li>• cannot contain the Grave accent character</li><li>• cannot contain the space character</li><li>• cannot have 4 or more repeating characters</li><li>• users cannot change a password more than once during a 24 hour period</li></ul>
Confirm Password	Confirm the password for the user.
Space	This field is not configurable. It is set to the global space.
Email	Enter the user's email address.

**TABLE 21.** ADD NEW USER FIELDS (CONT.)

Fields	Description
EDIPI	<p>Department of Defense customers only:</p> <p>Enter the user's the Department of Defense identification number, also known as the Electronic Data Interchange Personal Identifier.</p> <p>This field is required if your configuration on <b>Security &gt; Advanced &gt; Portal Authentication</b> specifies certificate authentication for access to the System Manager using a common access card (CAC).</p>

**Related topics**

["Advanced: Portal Authentication" on page 104](#)

**Editing local System Manager users****Procedure**

1. Log into the System Manager.
2. Select **Security > Identity Source > Local Users**.
3. Select the user ID of the entry to display the information for that user.
4. Make your changes.

Refer to ["Add New User window" on the previous page](#) table for details.

You cannot change the user ID.

5. Click **Apply > OK**.

**Deleting local System Manager users****Procedure**

1. Log into the System Manager.
2. Select **Security > Identity Source > Local Users**.
3. Select one or more check boxes for the users you want to delete.

4. Click **Delete**.

You cannot delete the user you logged in with.

5. Click **Yes > OK**.

## Certificate Mgmt

Use the **Security > Certificate Mgmt** menu items to fulfill certificate requirements your organization may have for the Ivanti EPMM appliance or the MDM client. With these options, you can:

- Generate a self-signed certificate
- Generate a CSR for a certificate authority
- Upload required certificates
- Enable certificate pinning



When you update a certificate, you are prompted to confirm that you want to proceed because the HTTP service needs to be restarted, resulting in service disruption.

---

This section includes the following topics:


- ["Certificates you configure in the System Manager" below](#)
- ["Generate a self-signed certificate" on page 62](#)
- ["Certificate signing request \(CSR\) requirements" on page 63](#)
- ["Generate a certificate signing request \(CSR\)" on page 63](#)
- ["Upload client certificate \(CSR\) window" on page 64](#)
- ["Uploading certificates" on page 65](#)
- ["Cert pinning for in-app registrations for iOS and Android devices" on page 65](#)
- ["Viewing certificates" on page 67](#)
- ["Access Control Lists: Networks and Hosts" on page 68](#)

## Certificates you configure in the System Manager

You configure the following certificates on the System Manager at **Security > Certificate Mgmt**:

Ivanti recommends to allow HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for EPMM server management and must have strictly controlled access.

**TABLE 22.** CERTIFICATES YOU CONFIGURE IN THE SYSTEM MANAGER

Certificate	
Portal HTTPS  Port 443 and 8443	<ul style="list-style-type: none"> <li>• The identify certificate and its certificate chain, including the private key, that identifies Ivanti EPMM, allowing a client (such as a browser or app) to trust Ivanti EPMM.</li> <li>• Used on port 8443 for the System Manager.</li> <li>• Must be a publicly trusted certificate from a well-known Certificate Authority if you are using mutual authentication.</li> <li>• Used on port 443 for these clients:               <ul style="list-style-type: none"> <li>◦ the Admin Portal</li> <li>◦ the self-service user portal.</li> <li>◦ Mobile@Work for iOS and Android device check-ins when using mutual authentication</li> <li>◦ Mobile@Work for macOS device check-ins</li> <li>◦ iOS MDM and macOS MDM check-ins</li> <li>◦ Windows device check-ins</li> <li>◦ Apps@Work on Android and iOS</li> </ul> </li> <li>• Typically the same certificate as the Client TLS and iOS Enrollment certificates.</li> <li>• Presented to client as part of the TLS handshake when client initiates a request to Ivanti EPMM.</li> </ul> <hr/> <div data-bbox="483 1203 537 1262"></div> <div data-bbox="570 1199 1393 1272">           Mobile@Work Clients require that the portal HTTPS certificate support either CRLs (Certificate Revocation Lists) or OCSP.         </div>
Client transport layer security (TLS)  Port 9997	<ul style="list-style-type: none"> <li>• The identify certificate and its certificate chain, including the private key, that identifies Ivanti EPMM, allowing Mobile@Work for iOS and Android to trust Ivanti EPMM.</li> <li>• Used on port 9997 for Mobile@Work for iOS and Android device check-ins when not using mutual authentication.</li> <li>• Typically the same certificate as the Portal HTTPS and iOS Enrollment certificates.</li> <li>• Presented to Mobile@Work for iOS or Android as part of the TLS handshake when Mobile@Work initiates a request to Ivanti EPMM.</li> </ul>

**TABLE 22.** CERTIFICATES YOU CONFIGURE IN THE SYSTEM MANAGER (CONT.)

Certificate	
	<ul style="list-style-type: none"> <li>Beginning September 1, 2020, Apple requires that valid Transport Layer Security (TLS) certificates expire in 397 days or less. From Ivanti EPMM 10.8.0.0 through the latest release supported by Ivanti, the lifespan of self-signed TLS certificates are limited to fewer than 398 days.</li> </ul>
iOS Enrollment	<ul style="list-style-type: none"> <li>The identify certificate and its certificate chain, including the private key, that identifies Ivanti EPMM. Ivanti EPMM uses the identity certificate to sign the Apple MDM configurations that it sends to iOS and macOS devices.</li> <li>Typically the same certificate as the Client TLS and Portal HTTPS certificates.</li> </ul>
Splunk certificate	<p>Configure the Splunk Client certificate in the Ivanti System Manager at <b>Security &gt; Certificate Mgmt &gt; Splunk Client certificate</b>.</p> <p>Configure the Splunk server certificate in Ivanti System Manager at <b>Data export&gt; Splunk indexer page</b>.</p>

## Generate a self-signed certificate

You can generate a self-signed certificate for:

- The Ivanti iOS Mobility Management Best Practices
- The Ivanti Sentry configurations
- The Portal HTTPS certificate, the Client TLS certificate, or the iOS Enrollment certificate.

### Procedure

- Log into System Manager.
- Go to Security > Certificate Mgmt.
- Select Manage Certificate in either the Portal HTTPS row, the Client TLS row, or the iOS Enrollment row.
- Select Certificate Options > Generate Self-Signed Certificate.

5. Click one of the following self-signed certificate options:

- Generate Self Signed RSA Certificate
- Generate Self Signed ECDSA Certificate

## Certificate signing request (CSR) requirements

The following table summarizes the requirements and related information for each component of an Ivanti EPMM deployment.

**TABLE 23.** CSR REQUIREMENTS

Component	Requirements
Appliance	<ul style="list-style-type: none"><li>• Private key file</li><li>• Certificate file</li><li>• Root CA certificate file</li><li>• Without password</li></ul>
Standalone Sentry	<ul style="list-style-type: none"><li>• Private key file</li><li>• Certificate file</li><li>• Root CA certificate file</li><li>• Without password</li></ul>
Client	<ul style="list-style-type: none"><li>• Private key file</li><li>• Certificate file</li><li>• Root CA certificate file</li><li>• Without password</li></ul>

## Generate a certificate signing request (CSR)

### Procedure

1. Log into System Manager.
2. Go to **Security > CertificateMgmt.**
3. Select **Manage Certificate** in either the **PortalHTTPS** row, the **ClientTLS** row, or the **iOS Enrollment** row.
4. Select **Certificate Options > Generate CSR.**

5. Fill in the form, as necessary. Refer to ["Upload client certificate \(CSR\) window" below](#) for details.
6. Click **Generate**.
7. Open a text file in a text editor or application.
8. Copy the content between BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST and paste it into the text file.
9. Open a second text file.
10. Copy the content between BEGIN RSA PRIVATE KEY and END RSA PRIVATE KEY and paste it into the second text file.
11. Click **Close**.
12. Submit the text file you created in step 8.

## Upload client certificate (CSR) window

The following table summarizes fields and descriptions in the **Upload client certificate** window:

**TABLE 24.** UPLOAD CLIENT CERTIFICATE FIELDS

Fields	Description
Common Name	Enter the server host name.
E-Mail	Enter the email address of the contact person in your organization who should receive the resulting certificate.
Company	Enter the name of the company requesting the certificate.
Department	Enter the department requesting the certificate.
City	Enter the city in which the company is located.
State	Enter the state in which the company is located.
Country	Enter the two-character abbreviation for the country in which the company is located.
Key Length	Select 2048 or 3072 to specify the length of each key in the pair. Longer keys provide stronger security, but may impact performance.



## Uploading certificates

You can upload a certificate after you receive the CA certificate from the certifying authority.

### Procedure

1. Log into System Manager.
2. Go to **Security > Certificate Mgmt.**
3. Select **Manage Certificate** in either the **PortalHTTPS** row, the **ClientTLS** row, or the **iOS Enrollment** row.
4. Select **Certificate Options > Upload Certificate.**
5. Select a certificate based on the following information:

6.	Fields	Description
	Key file	The file created in "Uploading certificates" above in "Uploading certificates" above
	Server certificate	The CA certificate file you received from the certifying authority.
	CA certificate	A generic CA certificate file.

7. Click **Upload Certificate.**

## Cert pinning for in-app registrations for iOS and Android devices

Beginning with Ivanti EPMM 11.4.0.0 release, you can set up and configure certificate pinning to prevent man-in-the-middle attacks for in-app registration of iOS and Android devices. From the **Certificate Mgmt** page, you can create a **Pinned Server Certificate** policy to deliver a set of certificates that clients can expect an Ivanti EPMM server to present during check-in and similar traffic. This feature is applicable for post-first-time use, for continuous assurance that the client is connecting to the correct Ivanti EPMM.

If none of the certificates configured match the active certificate in use on the Ivanti EPMM server, then devices will strictly honor the pinning policy and fail to connect until a correction of the certificate pinning policy is sent.

This pinning policy supports multiple entries to enable a smooth transition when the Ivanti EPMM server's certificate is about to expire. Administrators can include the renewal certificate before it is active on the server and keep the expiring certificate in this policy for seamless transition to the renewed certificate. Ivanti recommends administrator to set up Ivanti EPMM system certificate expiration alerts to be warned when EPMM's server certificate is about to expire.

### Before you begin

Mutual authentication (also known as *certificate-based authentication*) must be enabled to use this feature. For more information, see "Mutual authentication between devices and Ivanti EPMM" in the Managing Certificates and Configuring Certificate Authorities chapter of the *Ivanti EPMM Device Management Guide* for your operating system.

### Procedure

1. Log into System Manager.
2. Go to **Security > Certificate Mgmt > Create a Pinning Request**.

FIGURE 1. CREATE A PINNING REQUEST MENU

#### Create a Pinning Request

The current portal certificate has already been added to the certificate pinning request below. Either now, or at any time, you may add certificates, such as before an expired certificate will be replaced by its renewal. Once all the certificates you wish to include in your pinning statement are in the table below, clicking the "Generate Pinning Request" button will generate a downloadable file which you will send to MobileIron Support for processing.

#### Certificates

Name	View Certificate	Validity
SampleName	<a href="#">View</a>	2020-09-21 5:00:00 PM To 2021-09-22 4:59:59 PM <a href="#">Delete</a>

[+ Add Certificate](#) **1**

Click below to download a Pinning Request for the Certificates listed above. You will need to send it to MobileIron Support for activation.

[Generate Pinning Request](#) **2**

Click below when you have received the activated Pinning Statement from MobileIron Support.

[Upload Pinning Statement](#) **3**

3. If you want to add any additional certificates to the ones listed, click the link **+Add Certificate** (caption 1). An **Upload Certificates** window opens.
4. Click **Choose File** and select the certificate you want to add.

- Click either **Add another file** or **Upload Certificate**. Any new certificates will display in the **Certificates** table.

FIGURE 2. CERTIFICATES TABLE WITH NEW SAMPLE CERTIFICATES

Certificates			
Name	View Certificate	Validity	
SampleName	<a href="#">View</a>	2020-09-21 5:00:00 PM To 2021-09-22 4:59:59 PM	<a href="#">Delete</a>
SampleName2	<a href="#">View</a>	2020-09-21 5:00:00 PM To 2021-09-22 4:59:59 PM	<a href="#">Delete</a>
<a href="#">+ Add Certificate</a>			

- To download a Pinning Request for the certificates in the table, click **Generate Pinning Request** (caption 2). This action initiates the download of a pinning statement request file in native Mac or Windows format.
- Contact your Support representative to submit the pinning request for activation.
- When you have received the activated Pinning Statement from Ivanti support, click **Upload Pinning Statement** (caption 3) to upload your pinning statement to Ivanti EPMM.
- To view your certificate, click **View** in the View Certificate column of the **Certificates** table.

## Viewing certificates

Use the **Security > Certificate Mgmt** menu items to view both Portal HTTPS or Client-TLS certificates.

### Procedure

- Log into System Manager.
- Go to **Security > Certificate Mgmt**.
- Select **View Certificate** in either the **PortalHTTPS** row, the **ClientTLS** row, or the **iOS Enrollment** row.
- To view certificate pinning certificates, click **View** in the View Certificate column of the **Certificates** table.

## Access Control Lists: Networks and Hosts

Use the **Security > Access Control Lists > Networks & Hosts** options to manage the servers and subnets you will use to compile Access Control Lists (ACLs) for Ivanti Clients.

This section includes the following topics:

- ["Adding a host or subnet mask" below](#)
- ["Add Network/Hosts window" below](#)

### Adding a host or subnet mask

Use the **Security > Access Control Lists > Networks & Hosts** options to add a host or subnet mask for compiling ACLs.

#### Procedure

1. Log into System Manager.
2. Go to **Security > Access Control Lists > Networks & Hosts**.
3. Click the **Add** to open the **Add Network/Host** window.
4. Modify one or more of the fields, as necessary.

Refer to ["Add Network/Hosts window" below](#) table for details.

5. Click **Apply > OK**.

This host or network will now be available for ACLs configured in the ACLs screen.

### Add Network/Hosts window

The following table summarizes fields and descriptions in the **Add Network/Hosts** window:

**TABLE 25.** ADD NETWORK/HOSTS FIELDS

Fields	Description
Name	Enter a name to use to identify this host or network.
Description	Enter additional text to provide supporting information about this host or network.

**TABLE 25.** ADD NETWORK/HOSTS FIELDS (CONT.)

Fields	Description
Type	Select Subnet or Host from the dropdown menu.
Network/Host	Enter the IP address for this network or host.

## Access Control Lists: Network Services

Use the **Security > Access Control Lists > Networks Services** options to manage available services. Ivanti EPMM pre-populates this list with common services.

This section includes the following topics:

- ["Adding a service" below](#)
- ["Add Network Services window" below](#)

### Adding a service

#### Procedure

1. Log into System Manager.
2. Go to **Security > Access Control Lists > Networks Services**.
3. Click **Add** to open the **Add Services** window.
4. Fill out the form, as required.

Refer to ["Add Network Services window" below](#) table for details.

5. Click **Apply > OK**.

### Add Network Services window

The following table summarizes fields and descriptions in the **Add Network Services** window:

**TABLE 26.** ADD NETWORK SERVICES FIELDS

Fields	Description
Name	Enter a name to use to identify this service.
Description	Enter additional text provide supporting information about this service.
Type	Select TCP, UDP, or IP from the drop-down menu.
Source Port	Enter the number of the source port for this service. Enter 0 to allow any source port.
Destination Port	Enter the number of the destination port for this service. Enter 0 to allow any destination port.

## Access Control Lists: ACLs

Use the **Security > Access Control Lists > ACLs** options to compile and manage the rules that define inbound and outbound access for network hosts and services.

Each ACL consists of one or more access control entries (ACEs). You need to complete the following tasks to configure ACLs:

1. Configure entries for each network and host requiring an ACL.
2. Configure entries for any network services requiring an ACL.
3. Create an ACL.

This section includes the following topics:

- ["Adding an ACL" below](#)
- ["Add ACL window" on the next page](#)
- ["Editing an ACL" on page 72](#)
- ["Copying an ACL" on page 72](#)
- ["Deleting an ACL" on page 72](#)

## Adding an ACL

### Procedure

1. Log into System Manager.
2. Go to **Security > Access Control Lists > ACLs**.

3. Click **Add** to open the **Add ACL** window.
4. Complete the form with the following information:
  - Name: Enter a name to use to identify this ACL.
  - Description: Enter additional text provide supporting information about this ACL.
5. Click **Submit** to enable the lower portion of the window and continue.
6. Click **Add** to add an access control entry (ACE) to the ACL.  
Each ACE consists of a combination of the network hosts and services you configured for use in ACLs.
7. Modify one or more of the fields, as necessary.  
Refer to ["Add ACL window" below](#) for details.
8. Click **Apply > OK**.

## Add ACL window

The following table summarizes fields and descriptions in the **Add ACL** window:

**TABLE 27.** ADD ACL FIELDS

Fields	Description
Source Network	Select the network from which access will originate. This list is populated with the networks and hosts you created for use with ACLs. See <a href="#">""Access Control Lists: Networks and Hosts" on page 68"</a> on <a href="#">"Access Control Lists: Networks and Hosts" on page 68</a> .
Destination Network	Select the network being accessed. This list is populated with the networks and hosts you created for use with ACLs. See <a href="#">""Access Control Lists: Networks and Hosts" on page 68"</a> on <a href="#">"Access Control Lists: Networks and Hosts" on page 68</a> .
Service	Select the network service to which this entry permits or denies access. This list is populated with the services you created for use with ACLs. See <a href="#">""Access Control Lists: Network Services" on page 69"</a> on <a href="#">"Access Control Lists: Network Services" on page 69</a> .
Action	Select <b>Permit</b> or <b>Deny</b> from the drop down list.
Connections Per Minute	Enter the number of connections to allow per minute.
Description	Enter text to describe the purpose of this entry.

## Editing an ACL

### Procedure

1. Log into System Manager.
2. Go to **Security > Access Control Lists > ACLs**.
3. Complete one or more of the following modifications to the ACL:
  - Select an ACL and click **Delete**.
  - Click **Add** to add an ACL.
  - Select the ACL above the new ACL and click **Insert**.
4. Click **Apply > OK**.

## Copying an ACL

### Procedure

To start a new ACL based on an existing one:

1. Log into System Manager.
2. Go to **Security > Access Control Lists > ACLs**.
3. Select the ACL you want to copy.
4. Click the **Copy** button.
5. Enter a name for the new ACL.
6. Click **OK > OK**.

## Deleting an ACL

### Procedure

1. Log into System Manager.
2. Go to **Security > Access Control Lists > ACLs**.



3. Select one or more of the check boxes next to an ACL you want to delete.
4. Click **Delete > Yes**.

## Access Control Lists: Portal ACLs

Use the **Security > Access Control Lists > Portal ACLs** options to further restrict access to various portals within Ivanti EPMM.

This section includes the following topics:

- ["Enabling an ACL Portal" below](#)
- ["Portal ACLs window" on the next page](#)

## Enabling an ACL Portal

### Procedure

1. Log into System Manager.
2. Go to **Security > Access Control Lists > Portal ACLs**.
3. Select the portal you want to enable.

Refer to ["Portal ACLs window" on the next page](#) for details.

4. Enter the IP address or network/mask pair to specify servers or networks that may access this component. Separate the entries with spaces.

Examples:

- 100.0.0.0 150.0.0.0
- 101.0.0.0 10.0.0.0/255.255.255.0

**You must use the expanded form of the mask. Do not** specify an entry similar to 10.0.0.0/24.

If your Ivanti EPMM is behind a NAT, enter the IP of the NAT network.

Remember that the Sentry must be able to access Ivanti EPMM. If it does not have access, then the ActiveSync Devices page will not display devices.

5. Click **Apply > OK**.

## Portal ACLs window

The following table summarizes fields and descriptions in the **Portal ACLs** window:

**TABLE 28.** PORTAL ACLS FIELDS

Fields	Description
User Portal	Enables device users to register their devices, view device information, and manage their devices.
Admin Portal	The Admin Portal.
System Manager Portal	The System Manager.
Sentry Connection	The Sentry installed for ActiveSync access control.
API Connection	The Web Services API.
iOS MDM	The iOS MDM service for profile management.
iOS iReg URL	The iReg service that enables provisioning iOS devices without installing the MI Go app.
OAuth API	Enables or disables the OAuth API. You can control access to the OAuth API by defining IP addresses, ranges of IP addresses and subnets based on the values they enter into the field. Addresses can be internal (non-routable) or external (routable). With this control, you can limit access to OAuth API from routable IP addresses or restrict access to specific machines for security reasons.
App Storefront Connection	The app management service for iOS.

## Advanced: Host Header Validation

Use the **Security > Advanced > Host Header Validation** options to enhance security of incoming HTTP traffic in Ivanti EPMM, by validating HTTP host headers. When you enable this feature, incoming HTTP host headers must contain either the specified internal hostname or the allowed external hostnames.

This section includes the following topics:

- ["Selecting host header validation" on the next page](#)
- ["Strict Host Header Validation options" on the next page](#)

## Selecting host header validation

### Procedure

To validate host headers in your Ivanti EPMM HTTP traffic:

1. Log into System Manager.
2. Go to **Security > Advanced > Host Header Validation**.
3. Go to the **Strict Host Header Validation** options.
4. Modify the fields, as necessary.

Refer to "[Strict Host Header Validation options](#)" below table for more information.

5. Click **Apply > OK**.

## Strict Host Header Validation options

The following table summarizes the **Strict Host Header Validation** options:

**TABLE 29.** STRICT HOST HEADER VALIDATION OPTIONS

Fields	Description
Enable Strict Host Header Validation	Check this option to enable HTTP host header validation.
Internal Server Names	The internal server name is displayed.
External Server Name	(Optional) Specify one or more external server names that are trusted in the HTTP host header.

## Advanced: HSTS

Use **Security > Advanced > HSTS** to enable HTTP Strict Transport Security (HSTS). HSTS provides an additional layer of security for HTTPS. It helps prevent man-in-the-middle attacks by greatly reducing the ability to intercept requests and responses between a user and a web application server.

When you enable HSTS on Ivanti EPMM, web browsers enforce a secure HTTPS connection for all communication with Ivanti EPMM. If Ivanti EPMM uses a self-signed certificate or if the portal certificate on Ivanti EPMM has expired, a warning message is displayed in the browser and users cannot access the resource. Users do not have the option to bypass the warning message to access the resource. By default, HSTS is disabled.

Ivanti recommends caution before enabling HSTS. Enabling HSTS may cause browsers to block access to Ivanti EPMM resources if a self-signed certificate is in use or the certificate has expired.

The following Ivanti EPMM services are impacted by HSTS:

- Ivanti Admin Portal
- Ivanti EPMM System Manager
- Self-Service User Portal

When you enable HSTS, provisional protocol access over port 8080 must be disabled. Access will be allowed only for HTTPS over port 443.

This section includes the following topics:

- ["Before enabling HSTS" below](#)
- ["Enabling HSTS" on the next page](#)
- ["Disabling HSTS" on the next page](#)

## Before enabling HSTS

Before enabling HSTS ensure the following:

- Ivanti EPMM uses a root or intermediate certificate from a publicly trusted CA.
- You have policies and processes in place that ensure that the certificate is current and has not expired.
- Ensure that port 443 is open.
- Provisioning protocol must be set as HTTPS, and the provisioning port must be set as 443. Provisioning protocol and port are set in the Ivanti EPMM System Manager, under **Settings > Port Settings**.

## Enabling HSTS

### Procedure

1. Log into System Manager.
2. Go to **Security > Advanced > HSTS**.
3. Make the following selections:

**Status:** select **Enabled** from the drop down list.

**Max Age:** enter a number.

The number indicates, in seconds, the length of time HSTS will be enabled on the browser. After the set time, the browser will not enforce HSTS connections.

4. Click **Apply > OK**.

## Disabling HSTS

You can also disable HSTS using Ivanti EPMM command line interface (CLI). For information about using the Ivanti EPMM CLI to disable HSTS, see "hsts-disable" in the *Command Line Interface (CLI) Reference*.

### Procedure

1. Log into System Manager.
2. Go to **Security > Advanced > HSTS**.
3. Change the **Max Age** to 0.

When you set **Max Age** to 0, Ivanti EPMM sends the HSTS header with the 0 value to the browser. This effectively results in the expiration of the HSTS policy and allows immediate access without requiring trusted SSL certificates.

For additional information see [Security Bulletin: HTTP Strict Transport Security \(HSTS\) in Ivanti EPMM 9.0](#).

## Advanced: Incoming SSL Configuration

For incoming SSL/TLS connections, Ivanti EPMM supports:

- TLS protocol version TLS v1.2 (TLS v1.0 and TLS v1.1 are not supported)
- a default set of disabled and selected cipher suites.

Use the **Security > Advanced > Incoming SSL Configuration** options to configure the cipher suites to use for incoming SSL/TLS connections to Ivanti EPMM. These incoming connections include connections initiated to Ivanti EPMM from:

- devices
- browsers (to the Admin Portal or System Manager)
- external servers

Use this feature to also:

- configure Ivanti EPMM to be PCI-DSS 3.1 compliant.
- change the cipher suites for incoming SSL/TLS connections if you have specific security or performance requirements.



**Important** Do not change the cipher suites unless you have specific security or performance requirements. Most customers do not need to take any actions.

---

This section includes the following topics:

- ["Protocols and cipher suites on Ivanti EPMM first-time installation" below](#)
- ["Advanced: Incoming SSL Configuration" on the previous page](#)
- ["Protocol version negotiation for incoming SSL/TLS connections" on the next page](#)
- ["Verify server requirements for incoming SSL/TLS connections" on page 80](#)
- ["Configuring incoming SSL/TLS connections" on page 80](#)
- ["Changing to the default set of cipher suites for incoming connections" on page 81](#)

## Protocols and cipher suites on Ivanti EPMM first-time installation

On first-time installation, Ivanti EPMM supports:

- Protocol version **TLSv1.2**
- Default and selected cipher suites as displayed in the System Manager at **Security > Advanced > Incoming SSL Configuration**.


Do not change the cipher suites until you have determined the cipher suites required for incoming connections to Ivanti EPMM.

## Protocol versions for incoming connections on upgrade

When you upgrade to this Ivanti EPMM version, the selected and disabled protocol versions are as follows, *regardless what they were set to before the upgrade*:

- Selected: **TLSv1.2**
- Disabled: **None**

---

 **TLS v1.2** is the only supported protocol and cannot be moved to the disabled list.

---

## Cipher suites for incoming connections on upgrade

When upgrading to Ivanti EPMM, Ivanti EPMM uses the disabled and selected sets of cipher suites that you used in the Ivanti EPMM from which you upgraded. The exception to this rule is when an Ivanti EPMM release removes cipher suites. In that case, the removed cipher suites are no longer available to select after upgrade.

Note that Ivanti EPMM has a default set of selected and disabled cipher suites. Ivanti EPMM uses these default sets after upgrades only if you use the **Reset to Default** button. The default sets have changed in various Ivanti EPMM releases. Therefore, if your upgrade path took you through a release that changed the default sets, use the **Reset to Default** button **only with caution** as described in ["Changing to the default set of cipher suites for incoming connections" on page 81](#).

The default sets changed in:

- Ivanti EPMM 10.2.0.0
- Ivanti EPMM 10.3.0.0
- Ivanti EPMM 11.4.0.0

## Protocol version negotiation for incoming SSL/TLS connections


Because Ivanti EPMM supports only TLSv1.2, incoming SSL/TLS connections fail if they are from a server that does not support TLSv1.2.

## Verify server requirements for incoming SSL/TLS connections

Before changing cipher suites used for incoming connections to Ivanti EPMM, verify the requirements of external servers that make connection requests to Ivanti EPMM. The System Manager screen at **Security > Advanced > Incoming SSL Configuration** indicates which cipher suites are disabled and selected.

The **Disabled** and **Selected** sections are described below:

**TABLE 30.** DISABLED AND SELECTED LISTS

Fields	Description
<b>Disabled</b>	<p>The protocol or cipher suite is available in Ivanti EPMM, but it is disabled. Therefore, Ivanti EPMM will not use it in any incoming connections.</p> <p>Putting protocols and cipher suites in the <b>Disabled Column</b> disables them when the configuration is saved.</p> <hr/> <p> TLS v1.2 is the only supported protocol and cannot be moved to the disabled list.</p> <hr/>
<b>Selected</b>	<p>Ivanti EPMM can use the protocol or cipher suite in an incoming connection.</p> <p>Putting protocols and cipher suites in the <b>Selected Column</b> enables them when the configuration is saved.</p>

## Configuring incoming SSL/TLS connections

Ivanti recommends that you use the default cipher suites for incoming SSL/TLS connections. Most customers do not need to change them. However, if you have specific security or performance requirements, you can change the defaults. Before changing the cipher suites used in incoming SSL/TLS connections, understand the requirements of external servers that make connection requests to Ivanti EPMM.

## Prerequisites for configuring incoming SSL/TLS connections

The following conditions must be met to configure incoming SSL/TLS connections:



- Configure incoming SSL/TLS connections only from the primary Ivanti EPMM for HA configurations. Configuring incoming SSL/TLS connections from the second or third instance of Ivanti EPMM is not supported since the Tomcat service will not be running in the second and third Ivanti EPMM.
- The administrator (local user) configuring the incoming SSL/TLS connections in the System Manager must also be an administrator (local user) in the Admin Portal.

## Configuring the cipher suites for incoming SSL/TLS connections

You can configure the cipher suites for incoming SSL/TLS connections.



You cannot disable the protocol TLSv1.2. If you move it to the **Disabled** list and click **Apply**, Ivanti EPMM displays an error message. Move TLSv1.2 back to the **Selected** list before re-clicking **Apply**.

---

### Procedure

1. Log into System Manager.
2. Go to **Security > Advanced > Incoming SSL Configuration**.
3. Go to the **Cipher Suites** section.
4. Click and drag, or select and move using the arrows, cipher suites between the **Disabled** and **Selected** lists to select the cipher suites to use for incoming SSL/TLS connections.
5. List the cipher suites in order, from highest preference to lowest by dragging each cipher suite up or down in the **Selected** list.

Ivanti EPMM uses the listed order in determining which, of the supported cipher suites, to use. Therefore, Ivanti suggests you list the strongest cipher suites first.

6. Click **Apply > OK**.

Ivanti EPMM Tomcat service, which supports web requests to and from Ivanti EPMM, restarts automatically.

## Changing to the default set of cipher suites for incoming connections

When you upgrade Ivanti EPMM, the set of incoming SSL/TLS protocols and cipher suites are the ones described in ["Advanced: Incoming SSL Configuration" on page 77](#).

You can change your cipher suite set to a set of your choice. You can also change to the default Ivanti EPMM set using the **Reset to Default** on the System Manager's **Security > Advanced > Incoming SSL Configuration** screen.

Most customers do not need to make any changes. However, you can change Ivanti EPMM to use the Ivanti EPMM default set of cipher suites if you have specific security requirements.

**Do not click Reset to Default unless:**

- You have specific security or performance requirements to use the Ivanti EPMM set of cipher suites. Most customers do not need to take any action.
- You have identified the cipher suites required for your external servers, and have confirmed that they are included in the default set of cipher suites.

For example, after an upgrade, an external server that depends on a legacy cipher suite that is not in the default set of cipher suites can connect to Ivanti EPMM. However, after you click **Reset to Default**, that server will not be able to connect to Ivanti EPMM.

**Procedure**

To change the configuration to the Ivanti EPMM default set of cipher suites:

1. Log into System Manager.
2. Go to **Security > Advanced > Incoming SSL Configuration**.
3. Click **Reset to Default**.
4. Click **Apply > OK**.

Ivanti EPMM Tomcat service, which supports web requests to and from Ivanti EPMM, restarts automatically.

## Advanced: Outgoing SSL Configuration

For outgoing SSL/TLS connections, Ivanti EPMM supports:

- TLS protocol version TLS v1.2 (TLS v1.0 and TLS v1.1 are not supported)
- A default set of disabled and selected cipher suites.

Use the **Security > Advanced > Outgoing SSL Configuration** options to configure the cipher suites to use for outgoing SSL/TLS connections from Ivanti EPMM to external servers. Use this feature to also:

- Configure Ivanti EPMM to be PCI-DSS 3.1 compliant
- Change the cipher suites and for outgoing SSL/TLS connections if you have particular security or performance requirements

The configuration impacts connections to all external servers. Examples of external servers are SCEP servers and Apple Push Notification Service (APNS).



**Important** Do not change the cipher suites unless you have specific security or performance requirements. Most customers do not need to take any actions.

---

Ivanti EPMM uses a Server Name Extension (SNI) when making outgoing TLS connections. SNI is used by TLS clients (in this case Ivanti EPMM) to indicate to a TLS server which hostname the client is attempting to reach. In the case where a single server is responding to multiple hostnames, using a SNI allows the server to respond with the correct TLS certificate to match the client's request. No Ivanti EPMM configuration is required for using SNI.

This section includes the following topics:

- ["Protocols and cipher suites on Ivanti EPMM first-time installation" below](#)
- ["Protocols and cipher suites on Ivanti EPMM upgrades" on the next page](#)
- ["Protocol version negotiation for outgoing SSL/TLS connections" on page 85](#)
- ["Determining which servers use which protocol versions and cipher suites" on page 85](#)
- ["Configuring outgoing SSL/TLS connections" on page 87](#)
- ["Changing to the default set of cipher suites for outgoing connections" on page 88](#)
- ["External servers connected to with outgoing SSL connections" on page 89](#)

## Protocols and cipher suites on Ivanti EPMM first-time installation

On first-time installation, Ivanti EPMM supports:

- Protocol version TLSv1.2
- Default and selected cipher suites as displayed in the System Manager at **Security > Advanced > Outgoing SSL Configuration**.

Do not change the cipher suites until you have determined the cipher suites required for your external servers. See ["Determining which servers use which protocol versions and cipher suites" on page 85](#) for details.

## Protocols and cipher suites on Ivanti EPMM upgrades

### Protocol versions for outgoing connections on upgrade

When you upgrade to this Ivanti EPMM version, the selected and disabled protocol versions are as follows, *regardless what they were set to before the upgrade*:

- Selected: TLSv1.2
- Disabled: None



TLS v1.2 is the only supported protocol and cannot be moved to the disabled list.

---

### Cipher suites for outgoing connections on upgrade

When upgrading Ivanti EPMM, Ivanti EPMM uses the disabled and selected sets of cipher suites that you used in the Ivanti EPMM from which you upgraded. The exception to this rule is when an Ivanti EPMM release removes cipher suites. In that case, the removed cipher suites are no longer available to select after upgrade.

Note that Ivanti EPMM has a default set of selected and disabled cipher suites. Ivanti EPMM uses these default sets after upgrades only if you use the **Reset to Default** button. The default sets have changed in various Ivanti EPMM releases. Therefore, if your upgrade path took you through a release that changed the default sets, use the **Reset to Default** button **only with caution** as described in ["Changing to the default set of cipher suites for outgoing connections" on page 88](#).

The default sets changed in:

- Ivanti EPMM 10.2.0.0
- Ivanti EPMM 10.3.0.0
- Ivanti EPMM 11.4.0.0

### Related topics

- ["Determining which servers use which protocol versions and cipher suites" on the next page](#)
- ["Changing to the default set of cipher suites for outgoing connections" on page 88](#)

## Protocol version negotiation for outgoing SSL/TLS connections

Because Ivanti EPMM supports only TLSv1.2, outgoing SSL/TLS connections fail if they are to a server that does not support TLSv1.2.

## Determining which servers use which protocol versions and cipher suites

Ivanti EPMM uses only the TLSv1.2 protocol for outgoing connections to external servers. If an external server is not configured to use TLSv1.2, connections to it from Ivanti EPMM will fail. Change the external server to use TLSv1.2.

Ivanti provides a utility that can determine the TLS protocols used in outgoing connections. See [https://help.ivanti.com/mi/help/en\\_US/CORE/10.7.0.1/rn/Content/CoreConnectorReleaseNotes/TLS%20Protocols%20Disabled.htm](https://help.ivanti.com/mi/help/en_US/CORE/10.7.0.1/rn/Content/CoreConnectorReleaseNotes/TLS%20Protocols%20Disabled.htm)

Regarding cipher suites, before you change which cipher suites to use to connect with external servers, make sure you know what the external servers require.

The System Manager screen at **Security > Advanced > Outgoing SSL** can help inform you of this information.

The **Disabled** and **Selected** lists mean the following:

**TABLE 31.** AVAILABLE AND SELECTED LISTS

Fields	Description
<b>Disabled</b>	<p>The cipher suite is available in Ivanti EPMM, but it is disabled. Therefore, Ivanti EPMM will not use it in any connections to external servers.</p> <p>If the cipher suite is colored red, it is a legacy cipher suite that was in an Ivanti EPMM version in your upgrade path. It is not in the set of the current Ivanti EPMM version.</p>
<b>Selected</b>	<p>Ivanti EPMM can use the cipher suite in a connection to an external server.</p> <p>If the cipher suite is colored red, it is a legacy cipher suite that was in an Ivanti EPMM version in your upgrade path. It is not in the set of the current Ivanti EPMM version.</p>

An asterisk (\*) on a protocol or cipher suite means the following:

**TABLE 32.** ASTERISK, PROTOCOL, CIPHER SUITE

Asterisk (*)	Description
Asterisk ( <b>*</b> ) on a <b>Disabled</b> cipher suite protocol	<p>The cipher suite is required by an external server. A connection attempt failed because the external server does not support any of the selected cipher suites.</p> <p>Hover your mouse over the cipher suite. The display lists the external servers to which connections failed because that protocol or cipher suite was not in the <b>Selected</b> set.</p> <p><b>Example</b></p> <p>2 endpoints have negotiated this protocol or cipher since 4 Feb 2020 01:53:04 GMT</p> <p>Endpoints:</p> <ul style="list-style-type: none"> <li>mdmenrollment.apple.com/17.146.232.35:443</li> <li>accounts.google.com/216.58.192.45:443</li> </ul>
Asterisk ( <b>*</b> ) on a <b>Selected</b> cipher suite or protocol	<p>The protocol or cipher suite was used in a connection to an external server.</p> <p>Hover your mouse over the protocol or cipher suite. The display lists the external servers that have connected to Ivanti EPMM using that protocol or cipher suite.</p> <p><b>Example</b></p> <p>1 endpoints have negotiated this protocol or cipher since 4 Feb 2020 01:53:04 GMT</p> <p>Endpoints:</p> <ul style="list-style-type: none"> <li>appgw.ivanti.com/199.127.91.250:443</li> </ul>

To populate the usage information indicated by the asterisks:

- Run Ivanti EPMM for a two or three days, giving time to attempt most outgoing SSL/TLS connections.
- In the Admin Portal, go to **Services > Overview** and click **Verify All**. This action makes connection attempts to many external servers.

After the usage information has been populated, you can determine:

- Cipher suites in the **Disabled** list that you must move to the **Selected** list because at least one external server requires it. Alternatively, you can reconfigure the external server to support a selected cipher suite.
- Cipher suites in the **Selected** list that you can move to the **Disabled** list, because no external servers use it. Typically, this is because you are using a stronger cipher suite.

## Notes

- Ivanti EPMM clears the asterisks and associated usage information once a week.
- The weekly collection period begins when you restart Ivanti EPMM, or when you click **Apply** to change the cipher suite choices.
- To see up-to-date asterisk information, click on **Security > Advanced > Outgoing SSL Configuration**.

## Configuring outgoing SSL/TLS connections

Ivanti recommends that you use the default cipher suites for outgoing SSL/TLS connections. Most customers do not need to change them. However, if you have specific security or performance requirements, you can change the choices. Before changing the cipher suites used in outgoing SSL/TLS connection, see ["Determining which servers use which protocol versions and cipher suites" on page 85](#) for details.

## Prerequisites for configuring outgoing SSL/TLS connections

The following conditions must be met to configure outgoing SSL/TLS connections:

- Configure outgoing SSL/TLS connections only from the primary Ivanti EPMM for HA configurations. Configuring outgoing SSL connections from the second or third instance of Ivanti EPMM is not supported since the Tomcat service will be down in the second and third Ivanti EPMM.
- The administrator configuring the outgoing SSL/TLS connections in the System Manager must also be an administrator in the Admin Portal.

## Configuring the cipher suites for outgoing SSL/TLS connections

You can configure the cipher suites for outgoing SSL/TLS connections.



You cannot disable the protocol TLSv1.2. If you move it to the **Disabled** list and click **Apply**, Ivanti EPMM displays an error message. Move TLSv1.2 back to the **Selected** list before re-clicking **Apply**.

## Procedure

To change the cipher suites for outgoing SSL/TLS connections:

1. Log into System Manager.
2. Go to **Security > Advanced > Outgoing SSL Configuration**.
3. Go to the **Cipher Suites** section.
4. Click and drag cipher suites between the **Disabled** and **Selected** lists to select the cipher suites to use for outgoing SSL/TLS connections.
5. List the cipher suites in order, from highest preference to lowest by dragging each cipher suite up or down in the **Selected** list.

Each external server uses the listed order in determining which cipher suite to use of the cipher suites that it supports. Therefore, Ivanti suggests you list the strongest cipher suites first.

6. Click **Apply > OK**.

Ivanti EPMM Tomcat service, which supports web requests to and from Ivanti EPMM, automatically restarts.

## Changing to the default set of cipher suites for outgoing connections

When you upgrade Ivanti EPMM, the set of outgoing SSL/TLS protocols and cipher suites on your Ivanti EPMM are the ones described in ["Protocols and cipher suites on Ivanti EPMM upgrades" on page 84](#).

You can change the cipher suite set to a set of your choice. You can also change to the default Ivanti EPMM set using the **Reset to Default** on the System Manager's **Security > Advanced > Outgoing SSL** screen.

Most customers do not need to make any changes. However, you can change Ivanti EPMM to use the Ivanti EPMM default set of cipher suites if you have specific security requirements.

**Do not click Reset to Default unless:**



- You have specific security or performance requirements to use the Ivanti EPMM set of cipher suites. Most customers do not need to take any action.
- You have identified the cipher suites required for your external servers, and have confirmed that they are included in the default set of cipher suites.

For example, after an upgrade, an external server that depends on a legacy cipher suite that is not in the default set of cipher suites can connect to Ivanti EPMM. However, after you click **Reset to Default**, that server will not be able to connect to Ivanti EPMM.

**Therefore, see ["Determining which servers use which protocol versions and cipher suites"](#) on page 85 before you click **Reset to Default**.**

### Procedure

To change the configuration to the Ivanti EPMM default set of strong cipher suites:

1. Log into System Manager.
2. Go to **Security > Advanced > Outgoing SSL Configuration**.
3. Click **Reset to Default**.
4. Click **Apply > OK**.

Ivanti EPMM Tomcat service, which supports web requests to and from Ivanti EPMM, restarts automatically.

## External servers connected to with outgoing SSL connections

Ivanti EPMM uses outgoing SSL/TLS connections to various external servers. Ivanti EPMM uses the TLSv1.2 protocol for these connections. If an external server is not configured to use TLSv1.2, change the external server to use TLSv1.2.

Some of these external servers are:

- Ivanti Standalone Sentry
- Connector
- SCEP servers
- LDAP servers
- Ivanti EPMM Gateway
- Apple Push Notification Service (APNS)
- Content Delivery Network servers
- Ivanti EPMM support server

- Outbound proxy for Gateway transactions and system updates
- SMTPS servers
- Public app stores (Apple, Google, Windows)
- Apple License servers
- Apple Device Enrollment servers
- Android for Work servers

### Related topics

- ["Determining which servers use which protocol versions and cipher suites" on page 85](#)
- ["Configuring outgoing SSL/TLS connections" on page 87](#)

## Advanced: ModSecurity

Use **Security > Advanced > ModSecurity** to enable an additional layer of protection against future security vulnerabilities. ModSecurity is an open source web application firewall ([www.modsecurity.org](http://www.modsecurity.org)). If certain types of public security vulnerabilities impact Ivanti EPMM in the future, Ivanti EPMM can notify customers to enable ModSecurity. In these cases, Ivanti EPMM will provide a URL of a rules file hosted by Ivanti. The file contains ModSecurity rules that protect Ivanti EPMM from security vulnerabilities and you can protect your Ivanti EPMM without upgrading to a new Ivanti EPMM release.



Do not enable ModSecurity unless Ivanti notifies you to do so.

---

This section includes the following topics:

- ["Enabling ModSecurity" below](#)
- ["Configuring Detection Only mode" on the next page](#)
- ["Viewing ModSecurity logs" on the next page](#)

## Enabling ModSecurity

If a future public security vulnerability impacts Ivanti EPMM, Ivanti will contact you to do the following:

### Procedure

1. Log into System Manager.
2. Go to **Security > Advanced > ModSecurity**.

3. Go to the **ModSecurity Configuration** options.
4. Set **Status** to **Enabled**.
5. Set **Remote Rule Server URL** to the URL that Ivanti provided to you.
6. Set **Audit Logging** to **Enabled**.

Enabling audit logging means any activity relating to the security vulnerability is logged.

7. Click **Apply > OK**.

## Configuring Detection Only mode

Sometimes Ivanti will direct you to configure ModSecurity to detect a specific type of attack on Ivanti EPMM without performing any action to block it.

### Procedure

1. Log into System Manager.
2. Go to **Security > Advanced > ModSecurity**.
3. Go to the **ModSecurity Configuration** options.
4. Set **Status** to **Detection Only**.
5. Set **Remote Rule Server URL** to the URL that Ivanti provided to you.
6. Set **Audit Logging** to **Enabled**.

Enabling audit logging means any activity relating to the security vulnerability is logged.

7. Click **Apply > OK**.

## Viewing ModSecurity logs

When you have enabled ModSecurity, or configured it in detection only mode, Ivanti EPMM logs related information.

## Procedure

1. Log into System Manager.
2. Go to **Security > Troubleshooting > Logs**.
3. Go to the **Export Logs** section.
4. Select **Show Tech**.
5. Go to **Type** and select **Download**.
6. Click **Download**.

The log files containing ModSecurity information are:

- modsec\_audit.log if you enabled ModSecurity
- error\_log.log if you configured ModSecurity in detection only mode

## Advanced: SAML

Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP).

Ivanti recommends to allow HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for EPMM server management and must have strictly controlled access.

This section contains the following topics:

- ["Configuring SAML/IdP support" on the next page](#)
- ["Deactivating or deleting the IdP metadata file" on page 94](#)

Use this feature to allow local administrator users to use single-sign on for the Admin Portal and self-service user portal. This feature also allows administrators to automatically redirect authentication for the Admin Portal and the user portal to your external IdP.

Enabling SAML restarts Ivanti EPMM, which disrupts services until the configuration is complete. Therefore, access to the Admin Portal and self-service user portal is not available until after the SAML/IdP configuration is successfully completed. Furthermore, username/password authentication and certificate authentication to the Admin Portal and the self-service user portal will be disabled.

SAML is not supported on the System Manager portal. However, when SAML is enabled, local users can authenticate to the System Manager with a user ID and password, but not with certificate authentication.



If you set up SAML after setting the Admin Portal to run on port 8443, automatic redirection to the Admin Portal and to the self-service user portal will succeed. If you set up SAML after setting the Admin Portal to 443 redirection will not succeed until you reconfigure the Admin Portal to run on port 8443.

Ivanti recommends to allow HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for EPMM server management and must have strictly controlled access.

---

You must reconfigure SAML using the System Manager if both of the following are true:

- You upgraded to this version of Ivanti EPMM from a version of Ivanti EPMM prior to 10.0.0.0.
- You had configured SAML using the command line on Ivanti EPMM. Note that configuring SAML from the command line is not supported from Ivanti EPMM 9.7 through the current Ivanti EPMM release.

Contact Ivanti Technical Support if you have authentication failures in this scenario.

## Configuring SAML/IdP support

This topic describes how to configure SAML over IdP. For more details, refer to Microsoft documentation.



Once set up for SAML on iReg or DEP devices, you will not be able to disable SAML from the System Manager. You must first de-select the "SAML-based registration" field in Ivanti EPMM's Device Registration page before you can disable the IdP SAML connection in the System Manager.

---

### Before you begin

- Create at least one SAML user, with associated permissions.
- Sign up with an external IdP.
- Be able to export the metadata file from the IdP.

### Procedure

1. Log into the System Manager Portal.
2. Go to **Security > Advanced > SAML**.

3. Click the box to **Enable** SAML.
4. Read the warning message and click **Yes** to restart Ivanti EPMM and turn on SAML. This can take a few minutes. The **Configuration Status** changes from **Restarting Tomcat...** to **In Progress**, followed by **Completed**.
5. Click **Download** to download the XML metadata file from Ivanti EPMM that was created as part of the Ivanti EPMM restart process.
6. Save this file locally.
7. After downloading and saving the metadata from Ivanti EPMM, upload the Ivanti EPMM metadata files to your IdP:
  - a. Export those metadata files from your idP, and upload them to Ivanti EPMM.
  - b. Click **Done** > **OK**.
  - c. Verify the IdP hostname/URL and modify it, if necessary. System Manager extracts the hostname or URL from the IdP metadata file and auto-populates these fields.
8. Click **Apply**.



If you do not complete configuring SAML, reboot Ivanti EPMM by selecting **Maintenance > Reboot > Reboot** in the System Manager.

---

## Deactivating or deleting the IdP metadata file

This topic describes how to deactivate or delete the SAML/IdP option.

### Procedure

1. Log into the System Manager Portal.
2. Go to **Security > Advanced > SAML**.
3. Click the box to **Disable** SAML to deactivate SAML or click **Delete** to delete the SAML file.

There is no option to delete the IdP metadata file - they upload a new one which replaces the previous one.

## Advanced: Outgoing SSL Configuration

For outgoing SSL/TLS connections, Ivanti EPMM supports:

- TLS protocol version TLS v1.2 (TLS v1.0 and TLS v1.1 are not supported)
- A default set of disabled and selected cipher suites.

Use the **Security > Advanced > Outgoing SSL Configuration** options to configure the cipher suites to use for outgoing SSL/TLS connections from Ivanti EPMM to external servers. Use this feature to also:

- Configure Ivanti EPMM to be PCI-DSS 3.1 compliant
- Change the cipher suites and for outgoing SSL/TLS connections if you have particular security or performance requirements

The configuration impacts connections to all external servers. Examples of external servers are SCEP servers and Apple Push Notification Service (APNS).



**Important** Do not change the cipher suites unless you have specific security or performance requirements. Most customers do not need to take any actions.

---

Ivanti EPMM uses a Server Name Extension (SNI) when making outgoing TLS connections. SNI is used by TLS clients (in this case Ivanti EPMM) to indicate to a TLS server which hostname the client is attempting to reach. In the case where a single server is responding to multiple hostnames, using a SNI allows the server to respond with the correct TLS certificate to match the client's request. No Ivanti EPMM configuration is required for using SNI.

This section includes the following topics:

- ["Protocols and cipher suites on Ivanti EPMM first-time installation" below](#)
- ["Protocols and cipher suites on Ivanti EPMM upgrades" on the next page](#)
- ["Protocol version negotiation for outgoing SSL/TLS connections" on page 97](#)
- ["Determining which servers use which protocol versions and cipher suites" on page 97](#)
- ["Configuring outgoing SSL/TLS connections" on page 99](#)
- ["Changing to the default set of cipher suites for outgoing connections" on page 100](#)
- ["External servers connected to with outgoing SSL connections" on page 101](#)

## Protocols and cipher suites on Ivanti EPMM first-time installation

On first-time installation, Ivanti EPMM supports:

- Protocol version TLSv1.2
- Default and selected cipher suites as displayed in the System Manager at **Security > Advanced > Outgoing SSL Configuration**.

Do not change the cipher suites until you have determined the cipher suites required for your external servers. See ["Determining which servers use which protocol versions and cipher suites" on the next page](#) for details.

## Protocols and cipher suites on Ivanti EPMM upgrades

### Protocol versions for outgoing connections on upgrade

When you upgrade to this Ivanti EPMM version, the selected and disabled protocol versions are as follows, *regardless what they were set to before the upgrade*:

- Selected: TLSv1.2
- Disabled: None



TLS v1.2 is the only supported protocol and cannot be moved to the disabled list.

---

### Cipher suites for outgoing connections on upgrade

When upgrading Ivanti EPMM, Ivanti EPMM uses the disabled and selected sets of cipher suites that you used in the Ivanti EPMM from which you upgraded. The exception to this rule is when an Ivanti EPMM release removes cipher suites. In that case, the removed cipher suites are no longer available to select after upgrade.

Note that Ivanti EPMM has a default set of selected and disabled cipher suites. Ivanti EPMM uses these default sets after upgrades only if you use the **Reset to Default** button. The default sets have changed in various Ivanti EPMM releases. Therefore, if your upgrade path took you through a release that changed the default sets, use the **Reset to Default** button **only with caution** as described in ["Changing to the default set of cipher suites for outgoing connections" on page 100](#).

The default sets changed in:

- Ivanti EPMM 10.2.0.0
- Ivanti EPMM 10.3.0.0
- Ivanti EPMM 11.4.0.0

### Related topics

- ["Determining which servers use which protocol versions and cipher suites" on the next page](#)
- ["Changing to the default set of cipher suites for outgoing connections" on page 100](#)



## Protocol version negotiation for outgoing SSL/TLS connections

Because Ivanti EPMM supports only TLSv1.2, outgoing SSL/TLS connections fail if they are to a server that does not support TLSv1.2.

## Determining which servers use which protocol versions and cipher suites

Ivanti EPMM uses only the TLSv1.2 protocol for outgoing connections to external servers. If an external server is not configured to use TLSv1.2, connections to it from Ivanti EPMM will fail. Change the external server to use TLSv1.2.

Ivanti provides a utility that can determine the TLS protocols used in outgoing connections. See [https://help.ivanti.com/mi/help/en\\_US/CORE/10.7.0.1/rn/Content/CoreConnectorReleaseNotes/TLS%20Protocols%20Disabled.htm](https://help.ivanti.com/mi/help/en_US/CORE/10.7.0.1/rn/Content/CoreConnectorReleaseNotes/TLS%20Protocols%20Disabled.htm)

Regarding cipher suites, before you change which cipher suites to use to connect with external servers, make sure you know what the external servers require.

The System Manager screen at **Security > Advanced > Outgoing SSL** can help inform you of this information.

The **Disabled** and **Selected** lists mean the following:

**TABLE 33.** AVAILABLE AND SELECTED LISTS

Fields	Description
<b>Disabled</b>	<p>The cipher suite is available in Ivanti EPMM, but it is disabled. Therefore, Ivanti EPMM will not use it in any connections to external servers.</p> <p>If the cipher suite is colored red, it is a legacy cipher suite that was in an Ivanti EPMM version in your upgrade path. It is not in the set of the current Ivanti EPMM version.</p>
<b>Selected</b>	<p>Ivanti EPMM can use the cipher suite in a connection to an external server.</p> <p>If the cipher suite is colored red, it is a legacy cipher suite that was in an Ivanti EPMM version in your upgrade path. It is not in the set of the current Ivanti EPMM version.</p>

An asterisk (\*) on a protocol or cipher suite means the following:

**TABLE 34.** ASTERISK, PROTOCOL, CIPHER SUITE

Asterisk (*)	Description
Asterisk ( <b>*</b> ) on a <b>Disabled</b> cipher suite protocol	<p>The cipher suite is required by an external server. A connection attempt failed because the external server does not support any of the selected cipher suites.</p> <p>Hover your mouse over the cipher suite. The display lists the external servers to which connections failed because that protocol or cipher suite was not in the <b>Selected</b> set.</p> <p><b>Example</b></p> <p>2 endpoints have negotiated this protocol or cipher since 4 Feb 2020 01:53:04 GMT</p> <p>Endpoints:</p> <ul style="list-style-type: none"> <li>mdmenrollment.apple.com/17.146.232.35:443</li> <li>accounts.google.com/216.58.192.45:443</li> </ul>
Asterisk ( <b>*</b> ) on a <b>Selected</b> cipher suite or protocol	<p>The protocol or cipher suite was used in a connection to an external server.</p> <p>Hover your mouse over the protocol or cipher suite. The display lists the external servers that have connected to Ivanti EPMM using that protocol or cipher suite.</p> <p><b>Example</b></p> <p>1 endpoints have negotiated this protocol or cipher since 4 Feb 2020 01:53:04 GMT</p> <p>Endpoints:</p> <ul style="list-style-type: none"> <li>appgw.ivanti.com/199.127.91.250:443</li> </ul>

To populate the usage information indicated by the asterisks:

- Run Ivanti EPMM for a two or three days, giving time to attempt most outgoing SSL/TLS connections.
- In the Admin Portal, go to **Services > Overview** and click **Verify All**. This action makes connection attempts to many external servers.

After the usage information has been populated, you can determine:

- Cipher suites in the **Disabled** list that you must move to the **Selected** list because at least one external server requires it. Alternatively, you can reconfigure the external server to support a selected cipher suite.
- Cipher suites in the **Selected** list that you can move to the **Disabled** list, because no external servers use it. Typically, this is because you are using a stronger cipher suite.

### Notes

- Ivanti EPMM clears the asterisks and associated usage information once a week.
- The weekly collection period begins when you restart Ivanti EPMM, or when you click **Apply** to change the cipher suite choices.
- To see up-to-date asterisk information, click on **Security > Advanced > Outgoing SSL Configuration**.

## Configuring outgoing SSL/TLS connections

Ivanti recommends that you use the default cipher suites for outgoing SSL/TLS connections. Most customers do not need to change them. However, if you have specific security or performance requirements, you can change the choices. Before changing the cipher suites used in outgoing SSL/TLS connection, see ["Determining which servers use which protocol versions and cipher suites" on page 97](#) for details.

### Prerequisites for configuring outgoing SSL/TLS connections

The following conditions must be met to configure outgoing SSL/TLS connections:

- Configure outgoing SSL/TLS connections only from the primary Ivanti EPMM for HA configurations. Configuring outgoing SSL connections from the second or third instance of Ivanti EPMM is not supported since the Tomcat service will be down in the second and third Ivanti EPMM.
- The administrator configuring the outgoing SSL/TLS connections in the System Manager must also be an administrator in the Admin Portal.

### Configuring the cipher suites for outgoing SSL/TLS connections

You can configure the cipher suites for outgoing SSL/TLS connections.



You cannot disable the protocol TLSv1.2. If you move it to the **Disabled** list and click **Apply**, Ivanti EPMM displays an error message. Move TLSv1.2 back to the **Selected** list before re-clicking **Apply**.

---

## Procedure

To change the cipher suites for outgoing SSL/TLS connections:

1. Log into System Manager.
2. Go to **Security > Advanced > Outgoing SSL Configuration**.
3. Go to the **Cipher Suites** section.
4. Click and drag cipher suites between the **Disabled** and **Selected** lists to select the cipher suites to use for outgoing SSL/TLS connections.
5. List the cipher suites in order, from highest preference to lowest by dragging each cipher suite up or down in the **Selected** list.

Each external server uses the listed order in determining which cipher suite to use of the cipher suites that it supports. Therefore, Ivanti suggests you list the strongest cipher suites first.

6. Click **Apply > OK**.

Ivanti EPMM Tomcat service, which supports web requests to and from Ivanti EPMM, automatically restarts.

## Changing to the default set of cipher suites for outgoing connections

When you upgrade Ivanti EPMM, the set of outgoing SSL/TLS protocols and cipher suites on your Ivanti EPMM are the ones described in ["Protocols and cipher suites on Ivanti EPMM upgrades" on page 96](#).

You can change the cipher suite set to a set of your choice. You can also change to the default Ivanti EPMM set using the **Reset to Default** on the System Manager's **Security > Advanced > Outgoing SSL** screen.

Most customers do not need to make any changes. However, you can change Ivanti EPMM to use the Ivanti EPMM default set of cipher suites if you have specific security requirements.

### Do not click Reset to Default unless:

- You have specific security or performance requirements to use the Ivanti EPMM set of cipher suites. Most customers do not need to take any action.
- You have identified the cipher suites required for your external servers, and have confirmed that they are included in the default set of cipher suites.

For example, after an upgrade, an external server that depends on a legacy cipher suite that is not in the default set of cipher suites can connect to Ivanti EPMM. However, after you click **Reset to Default**, that server will not be able to connect to Ivanti EPMM.

**Therefore, see ["Determining which servers use which protocol versions and cipher suites"](#) on page 97 before you click **Reset to Default**.**

### Procedure

To change the configuration to the Ivanti EPMM default set of strong cipher suites:

1. Log into System Manager.
2. Go to **Security > Advanced > Outgoing SSL Configuration**.
3. Click **Reset to Default**.
4. Click **Apply > OK**.

Ivanti EPMM Tomcat service, which supports web requests to and from Ivanti EPMM, restarts automatically.

### External servers connected to with outgoing SSL connections

Ivanti EPMM uses outgoing SSL/TLS connections to various external servers. Ivanti EPMM uses the TLSv1.2 protocol for these connections. If an external server is not configured to use TLSv1.2, change the external server to use TLSv1.2.

Some of these external servers are:

- Ivanti Standalone Sentry
- Connector
- SCEP servers
- LDAP servers
- Ivanti EPMM Gateway
- Apple Push Notification Service (APNS)
- Content Delivery Network servers
- Ivanti EPMM support server
- Outbound proxy for Gateway transactions and system updates
- SMTPS servers
- Public app stores (Apple, Google, Windows)
- Apple License servers
- Apple Device Enrollment servers
- Android for Work servers

### Related topics

- ["Determining which servers use which protocol versions and cipher suites" on page 97](#)
- ["Configuring outgoing SSL/TLS connections" on page 99](#)

## Advanced: Trusted Front End

Ivanti EPMM can support a TLS inspecting proxy using an Apache server to handle HTTPS requests from your devices to Ivanti EPMM when using mutual authentication. This proxy is also known as a Trusted Front End. It intercepts and decrypts HTTPS network traffic and when it determines that the final destination is Ivanti EPMM, it re-encrypts and forwards the traffic to Ivanti EPMM.

The devices that register to Ivanti EPMM (using port 443) must send HTTPS requests to the TFE rather than to Ivanti EPMM. Also, the TFE must be provisioned with digital certificates that establish an identity chain of trust with a legitimate server verified by a trusted third-party certificate authority.



If you are using SAML to allow local administrator users to use single-sign on for the Admin Portal and self-service user portal, after IDP authentication, the user is redirected to Ivanti EPMM's URL, not the Trusted Front End's URL. The Trusted Front End is only for communication with devices.

---

If you are not using an Apache server for your Trusted Front End, work with Ivanti Professional Services or an Ivanti certified partner to determine if you can set up this deployment.

## Ivanti Standalone Sentry to Ivanti EPMM mutual authentication using a TFE

Ivanti EPMM supports mutual authentication with Sentry using a Trusted Front End (TFE) from the following releases:

- **Ivanti EPMM** - 11.5.0.0 and newer versions
- **Standalone Sentry** - 9.15.0 and newer versions

Ivanti EPMM will only initiate mutual authentication if Sentry is running 9.15.0 or newer software.

### Before you begin

Work with Ivanti Professional Services or an Ivanti certified partner to set up this deployment.

1. Enable mutual authentication for Apple and Android devices as described in "Mutual authentication between devices and Ivanti EPMM" in the *Ivanti EPMM Device Management Guide*.
2. In your devices' sync policies in the Admin Portal, set **Server IP/Host Name** to your Trusted Front End. This configuration makes devices send requests to the Trusted Front End instead of Ivanti EPMM.
3. If you use an external host, which is configured in the Admin Portal, in **Settings > General > Enterprise**, make sure your external host is configured to forward requests to the Trusted Front End. Changing the external host requires an Ivanti EPMM restart, which you can do in the System Manager, in **Maintenance > Reboot**.
4. Set up your Trusted Front End to forward HTTPS requests from devices on port 443 to Ivanti EPMM.

### Procedure

1. In **Security > Advanced > Trusted Front End**, select **Enable TFE use for communication from devices to Ivanti EPMM**.
2. Click **Apply**.
3. Click **Download CA Certificates**.

A file called **tfe-ca-certs.zip** downloads. It contains the certificates that establish an identity chain of trust with a legitimate server verified by a trusted third-party certificate authority. These certificates allow the Trusted Front End and Ivanti EPMM to validate the identity certificate that the device presents.

4. Provision your Trusted Front End with the downloaded certificates.
5. Enter the following configuration choices when configuring TFE for your web server:
  - ProxyPreserveHost: **On**
  - RewriteEngine: **On**

Your Ivanti contact has an example configuration file for Apache called **ssl.conf**. If you are using the Apps@Work web clip for iOS devices, and you are using it on a port other than 7443, modify the value 7443 in ssl.conf.

6. Install **ssl.conf** on your Trusted Front End.

### Related topics:

"Mutual authentication between devices and Ivanti EPMM" in the *Ivanti EPMM Device Management Guide*.

## Advanced: Portal Authentication

Use **Security > Advanced > Portal Authentication** to set up the authentication method for:

- device users to access the self-service user portal
- administrators to access the Admin Portal
- administrators to access the System Manager



The authentication methods provided on this screen are not available if you enable SAML in the System Manager in **Security > Advanced > SAML**. For the Admin Portal and self-service user portal, authentication uses SAML. For the System Manager, local users authenticate to the System Manager using a user ID and password.

### Related topics

- ["Self-service user portal authentication" on the next page](#)
- ["Admin Portal authentication" on the next page](#)
- ["Certificates required for certificate authentication to Ivanti EPMM portals" on page 107](#)
- ["Certificate attribute mapping used in certificate authentication to the Ivanti EPMM portals" on page 107](#)
- ["Using \\$EDIPIS in certificate authentication" on page 110](#)
- ["Entrust URL for getting derived credentials" on page 110](#)
- ["Configuring password authentication to an Ivanti EPMM portal" on page 111](#)
- ["Configuring certificate authentication to the user portal" on page 111](#)
- ["Configuring certificate authentication to the Admin Portal" on page 113](#)
- ["Configuring certificate authentication to the System Manager" on page 114](#)
- ["Configuring the Entrust URL for getting derived credentials" on page 115](#)
- ["Replacing the certificate for authentication" on page 116](#)



## Self-service user portal authentication

Device users can authenticate to the self-service user portal using one or both of the following methods, according to how you configure Ivanti EPMM:

- a user name and password

These are the credentials a device user uses to register a device with Ivanti EPMM. This authentication method is the default.

- an identity certificate from a smart card

When using this authentication method, you can also set up the Entrust URL for getting derived credentials.

See "User portal authentication options" in the ***Device Management Guide*** for supported platforms for authenticating with a smart card.



Certificate authentication is also supported in FIPS mode.

---

The device user can be:

- an LDAP user
- an Admin Portal local user as set up in the Admin Portal in **Devices & Users > Users**.

### Related topics

- ["Configuring password authentication to an Ivanti EPMM portal" on page 111](#)
- ["Configuring certificate authentication to the user portal" on page 111](#)

## Admin Portal authentication

Admin Portal administrators are set up as local users in the Admin Portal in **Devices & Users > Users**. They can authenticate to the Admin Portal using one or both of the following methods, according to how you configure Ivanti EPMM:

- a user name and password

These are the credentials for the local user as set up in the Admin Portal in **Devices & Users > Users**. This authentication method is the default.

- an identity certificate from a smart card

See "Logging in to the Admin Portal with a smart card" in ***Getting Started with Ivanti EPMM*** for supported platforms for authenticating with a smart card.



Certificate authentication is also supported in FIPS mode.

---

### Related topics

- ["Configuring password authentication to an Ivanti EPMM portal" on page 111](#)
- ["Configuring certificate authentication to the Admin Portal" on page 113](#)

## System Manager authentication

System Manager administrators are set up as local users in the System Manager in **Security > Local Users**. They can authenticate to the System Manager using one or both of the following methods, according to how you configure Ivanti EPMM:

- a user name and password

These are the credentials for the local user as set up in the System Manager in **Security > Local Users**. This authentication method is the default.

- an identity certificate from a smart card

Using an identity certificate from a smart card is supported only on desktop computers. It is not supported on mobile devices. Also, it is not supported with Firefox.



Certificate authentication is also supported in FIPS mode.

---

### Related topics

- ["Configuring password authentication to an Ivanti EPMM portal" on page 111](#)
- ["Configuring certificate authentication to the Admin Portal" on page 113](#)

## Certificates required for certificate authentication to Ivanti EPMM portals

To allow certificate authentication to Ivanti EPMM portals (the Admin Portal, the System Manager, and the self-service user portal), use the Ivanti EPMM System Manager to upload a PEM-formatted file to Ivanti EPMM. The PEM-formatted file contains either:

- the issuing certificate authority (CA) certificate
- the supporting certificate chain

Ivanti EPMM does not check the certificate's validity. Make sure the certificate that you upload is valid. That is, make sure it is not expired and not revoked.

When users sign in to an Ivanti EPMM portal, they provide an identity certificate from a smart card. The Ivanti EPMM portal authenticates the user's identity certificate against the certificate that you uploaded to Ivanti EPMM. The same uploaded certificate is used for authentication to all the Ivanti EPMM portals.



For authentication of local users, set the User ID of the local user to the user identity from the identity certificate.

---

### Related topics

- ["Configuring certificate authentication to the user portal" on page 111](#)
- ["Configuring certificate authentication to the Admin Portal" on page 113](#)
- ["Configuring certificate authentication to the System Manager" on page 114](#)

## Certificate attribute mapping used in certificate authentication to the Ivanti EPMM portals

When the user presents an identity certificate for authentication, Ivanti EPMM authenticates the identity certificate against the issuing CA certificate or certificate chain you uploaded to Ivanti EPMM. As part of that authentication, Ivanti EPMM makes sure the user identity in the identity certificate is a valid Ivanti EPMM user. You configure which field in the identity certificate and which Ivanti EPMM substitution variable must match.

Therefore, when you upload the certificate used for authenticating user's identity certificate, you also configure the following mapping information:

- which field from the identity certificate the authentication uses as the user identity. The choices are:
  - the NT Principal Name
  - the RFC822 email name

Your choice must match the Subject Alternative Name type you chose for generating the identity certificate.



For the NT Principal Name, Ivanti EPMM uses the User Principal Name in the Subject Alternative Name (SAN) in the identity certificate.

- the Ivanti EPMM substitution variable, against which the authentication compares the user identity.

Allowed variables depends on the Ivanti EPMM Portal as given in the following table:

**TABLE 35.** SUPPORTED VARIABLES IN IVANTI EPMM

Supported variables	Admin Portal and Self-Service User Portal	System Manager
\$USERID\$ (default)	Yes	Yes
\$EMAIL\$	Yes	Yes
\$USER_UPN\$	Yes	No
\$EDIPI\$  For the Department of Defense only. See <a href="#">"Using \$EDIPI\$ in certificate authentication" on page 110.</a>	No	Yes
\$USER_CUSTOM1\$	Yes	No
\$USER_CUSTOM2\$	Yes	No
\$USER_CUSTOM3\$	Yes	No
\$USER_CUSTOM4\$	Yes	No

Your choice depends on the Ivanti EPMM variable you chose to populate the Subject Alternative Name in the identity certificate.

- You can map up to two attributes. If a second attribute is configured, both fields in the identity certificate must match with the Ivanti EPMM substitution value.

## Note The Following

- The same user identity mapping to an Ivanti EPMM variable is used for authentication to both the user portal and the Admin Portal.
- You separately configure the user identity mapping to an Ivanti EPMM variable for System Manager authentication.
- Using \$USER\_UPN\$ and \$USER\_CUSTOM1\$ through \$USER\_CUSTOM4\$ is only applicable for LDAP users.
- Consider the case in which you specify the NT Principal Name as the field to use from the identity certificate, and you specify \$USERID\$, \$EMAIL\$, or \$USER\_UPN\$ as the Ivanti EPMM substitution variable to match. Ivanti EPMM accepts both of the following formats as a match:
  - DOMAIN\userid
  - userid@domain

That is, the NT Principal Name and the Ivanti EPMM substitution variable can have different formats, but match as long as the domain and userid match.

- Ivanti EPMM versions prior to 10.0.0.0 always compared the User Principal Name in the Subject Alternative Name in the identity certificate to Ivanti EPMM's list of values for the \$USERID\$ variable. It accepted as a match either of the formats DOMAIN\userid and userid@domain. If no match was found, Ivanti EPMM compared the RFC822 email address in the Subject Alternative Name to Ivanti EPMM's list of values for the \$EMAIL\$ variable. If you are upgrading from one of those prior Ivanti EPMM releases, Ivanti EPMM continues the same behavior until you apply a new configuration in the System Manager in **Security > Advanced > Portal Authentication**.
- If you use a custom LDAP variable (\$USER\_CUSTOM1\$ through \$USER\_CUSTOM4\$) to compare the user identity to, the variable must resolve to only one field from the certificate. Otherwise, the authentication will fail.

### Related topics

- ["Configuring certificate authentication to the user portal" on page 111](#)
- ["Configuring certificate authentication to the Admin Portal" on page 113](#)
- ["Configuring certificate authentication to the System Manager" on page 114](#)
- ["Using \\$EDIP\\$ in certificate authentication" on the next page](#)

## Using \$EDIPI\$ in certificate authentication

Using the Ivanti EPMM substitution variable \$EDIPI\$ is applicable only to Department of Defense customers. You enter it when adding a System Manager local user. The variable contains the Department of Defense identification number, also known as the Electronic Data Interchange Personal Identifier.

Therefore, if you are a Department of Defense customer setting up authentication to the System Manager using a certificate on a Common Access Card (CAC), you must follow these steps:

### Procedure

1. Enter a value into the EDIPI field when you create a System Manager local user.

Make sure the format of the \$EDIPI\$ value for each local user matches the format of the EDIPI value in the NT Principal Name in the user's identity certificate.

2. Use the \$EDIPI\$ variable as the attribute against which the authentication compares the user identity.

Although using \$EDIPI\$ is required for CAC cards, Ivanti EPMM does not enforce the selection when you configure portal authentication. Ivanti EPMM also does not ensure that you have entered a EDIPI value for the System Manager local users.

## Entrust URL for getting derived credentials

When using certificate authentication to the self-service user portal, you can set up Ivanti EPMM so that users can get their Entrust derived credentials when they get their Ivanti EPMM registration PIN. Specifically, in the System Manager, you provide Ivanti EPMM with the Entrust IdentityGuard Self-Service Module (SSM) URL. This URL is a deep link that points directly to the page on the Entrust self-service portal where a user can get a derived credential.

When the user requests a derived credential on the user portal, the user portal redirects the user to the URL you provided. The user interacts with the Entrust self-service portal to get a derived credential, after which the Entrust self-service portal redirects the user back to the Ivanti EPMM user portal. The user uses the PIV-D Entrust app on a mobile device to activate the derived credential.

### Related topics

*Ivanti Derived Credentials Guide for EPMM*

## Configuring password authentication to an Ivanti EPMM portal

You can configure the following:

- Allow device users to authenticate with their user name and password to the self-service user portal.
- Allow administrators to authenticate with their user name and password to the Admin Portal.



Authenticating to the Admin Portal is the default Ivanti EPMM setting.

---

### Procedure

1. Log into System Manager.
2. Go to **Security > Advanced > Portal Authentication**.
3. Select **Password Authentication**.
4. Under **Password Authentication**, select one or more of **Self-Service User Portal**, **Admin Portal**, or **System Manager**.
5. Click **Apply > OK**.

### Related topics

- ["Self-service user portal authentication" on page 105](#)

## Configuring certificate authentication to the user portal

You can allow device users to authenticate to the self-service user portal with the identity certificate on a smart card.

**Before you begin:** Have the PEM-formatted issuing CA certificate or certificate chain available to upload to Ivanti EPMM if you have not already uploaded it for authentication to another portal.

### Procedure

1. Log into System Manager.
  2. Go to **Security > Advanced Portal Authentication**.
  3. Select **Certificate Authentication**.
  4. Under **Certificate Authentication**, select **Self-Service User Portal**.
-

5. Click **Upload Issuing CA Certificate**, to open the **Upload Issuing CA Certificate** window.



Ivanti EPMM uses the same issuing CA certificate or certificate chain for authentication to all Ivanti EPMM portals. If you have already uploaded the file, skip this step. Continue to selecting certificate attribute mapping.

---

6. Click **Choose File**, and select the PEM-formatted file that contains either the issuing CA certificate or the supporting certificate chain.
7. Click **Upload Certificate > OK**.
8. In **Select Certificate Attribute Mapping**:
  - a. In the **Map from attribute** dropdown, select the user identity type in the identity certificate to use for authenticating the user.
  - b. In the **Map to attribute** dropdown, select the Ivanti EPMM variable with which to compare the user identity.



Ivanti EPMM uses the same attribute mapping for authentication to both the user portal and the Admin Portal. If you already set this mapping, skip this step.

---

9. Click **Apply > OK**.



**Important!** Clicking **Apply** changes Ivanti EPMM authentication behavior to compare the **Map from attribute** user identity type to the **Map to attribute** Ivanti EPMM variable. The behavior in Ivanti EPMM versions prior to 10.0.0.0 compared the User Principal Name to \$USERID\$ and the RFC822 email to \$EMAIL\$.

---

### Related topics

- ["Certificates required for certificate authentication to Ivanti EPMM portals" on page 107](#)
- ["Certificate attribute mapping used in certificate authentication to the Ivanti EPMM portals" on page 107](#)



## Configuring certificate authentication to the Admin Portal

You can allow administrators to authenticate to the Admin Portal with the identity certificate on a smart card.

**Before you begin:** Have the PEM-formatted issuing CA certificate or certificate chain available to upload to Ivanti EPMM if you have not already uploaded it for authentication to another portal.

### Procedure

1. Log into **System Manager**.
2. Go to **Security > Advanced > Portal Authentication**.
3. Select **Certificate Authentication**.
4. Under **Certificate Authentication**, select **Admin Portal**.
5. Click **Upload Issuing CA Certificate** to open the **Upload Issuing CA Certificate** window.



Ivanti EPMM uses the same issuing CA certificate or certificate chain for authentication to all Ivanti EPMM portals. If you have already uploaded the file, skip this step. Continue to selecting certificate attribute mapping.

---

6. Click **Choose File**, and select the PEM-formatted file that contains either the issuing CA certificate or the supporting certificate chain.
7. Click **Upload Certificate > OK**.
8. In **Select Certificate Attribute Mapping**:
  - a. In the **Map from attribute** dropdown, select the user identity type in the identity certificate to use for authenticating the user.
  - b. In the **Map to attribute** dropdown, select the Ivanti EPMM variable with which to compare the user identity.



Ivanti EPMM uses the same attribute mapping for authentication to both the user portal and the Admin Portal. If you already set this mapping, skip this step.

---

9. Click **Apply > OK**.



Ivanti EPMM uses the same attribute mapping for authentication to both the user portal and the Admin Portal. If you already set this mapping, skip this step.

---

### Related topics

- ["Certificates required for certificate authentication to Ivanti EPMM portals" on page 107](#)
- ["Certificate attribute mapping used in certificate authentication to the Ivanti EPMM portals" on page 107](#)

## Configuring certificate authentication to the System Manager

You can allow administrators to authenticate to the System Manager with the identity certificate on a smart card.

**Before you begin:** Have the PEM-formatted issuing CA certificate or certificate chain available to upload to Ivanti EPMM if you have not already uploaded it for authentication to another portal.

### Procedure

1. Log into System Manager.
2. Go to **Security > Advanced > Portal Authentication**.
3. Select **Certificate Authentication**.
4. Under **Certificate Authentication**, select **System Manager**.
5. Select **PIV** or **CAC**, depending on whether the identity certificate to authenticate is on a personal identity verification (PIV) card or common access card (CAC).
6. Click **Upload Issuing CA Certificate** to open the **Upload Issuing CA Certificate** window.



Ivanti EPMM uses the same issuing CA certificate or certificate chain for authentication to all Ivanti EPMM portals. If you have already uploaded the file, skip this step. Continue to selecting certificate attribute mapping.

---

7. Click **Choose File**, and select the PEM-formatted file that contains either the issuing CA certificate or the supporting certificate chain.
  8. Click **Upload Certificate > OK**.
-

9. In **Select Certificate Attribute Mapping**:
  - a. In the **Map from attribute** dropdown, select the user identity type in the identity certificate to use for authenticating the user.
  - b. In the **Map to attribute** dropdown, select the Ivanti EPMM variable with which to compare the user identity. If you selected **CAC** when choosing **CAC** versus **PIV**, you must select \$EDIPI\$.
10. Click **Apply > OK**.

#### Related topics

- ["Certificates required for certificate authentication to Ivanti EPMM portals" on page 107](#)
- ["Certificate attribute mapping used in certificate authentication to the Ivanti EPMM portals" on page 107](#)
- ["Using \\$EDIPI\\$ in certificate authentication" on page 110](#)

## Configuring the Entrust URL for getting derived credentials

**Before you begin:** Set up certificate authentication to the self-service user portal as described in ["Configuring certificate authentication to the user portal" on page 111](#). To configure the Entrust URL for getting derived credentials:

1. Log into System Manager.
2. Go to **Security > Advanced > Portal Authentication**.
3. Select **Derived Mobile Smart Credential (Self-Service User Portal Only)**.

The field **Entrust IdentityGuard SSM URL** appears.

4. Enter the Entrust IdentityGuard Self-Service Module (SSM) URL.

This URL is a deep link that points directly to the page on the Entrust self-service portal where a user can get a derived credential.

5. Click **Apply > OK**.

#### Related topics

- *Ivanti EPMM Derived Credentials Guide using the PIV-D Entrust App*

## Replacing the certificate for authentication

After you have uploaded a PEM-formatted file to Ivanti EPMM, you can replace it when necessary. For example, if the existing issuing CA certificate is about to expire, upload a replacement.



Ivanti EPMM uses the same issuing CA certificate or certificate chain for authentication to all Ivanti EPMM portals.

---

### Procedure

1. Log into System Manager.
2. Go to **Security > Advanced > Portal Authentication**.
3. Click **Replace CA Certificate**.
4. Click **Choose File**, and select the PEM-formatted file that contains either the replacement issuing CA certificate or the supporting certificate chain.
5. Click **Upload Certificate > OK**.
6. Click **Save > OK**.

### Related topics

- ["Certificates required for certificate authentication to Ivanti EPMM portals" on page 107](#)

## Advanced: SSH Configuration

Use **Security > Advanced > SSH Configuration** to configure ciphers, key exchange algorithms and hmacs. The System Manager portal allows you to upload the public keys then enable or disable public key and password authentications. By default, both **Public Key Authentication** and **Password Authentication** options are enabled and SSH configurations are applied to both SSH client and server. Configurations persist after a Backup and Restore procedure is completed.

When enabled, SSH public key authentication is attempted first. A valid public key for an authorized administrator account must be uploaded. Otherwise, password authentication is used.



The public key authentication is specified by the administrator and is valid only for the user uploading the key. For example, if <admin> is the user uploading the key, then ssh for admin@<ip> will be successful.

---

The default (non-FIPS) SSH, FIPS SSH, and CC (Common Criteria) SSH configurations have different sets of ciphers, key exchange algorithms, and hash-based message authentication code (HMAC) options, as described in ["Default SSH configuration" below](#), ["FIPS SSH configuration" below](#), and ["CC SSH configurations" on the next page](#).



You cannot ssh to a cluster, you must instead ssh to a specific instance.

## Default SSH configuration

The following table lists the available options for the default SSH configuration:

**TABLE 36.** DEFAULT SSH CONFIGURATION OPTIONS

Configuration	Available	Selected
Key Exchange Algorithms	<ul style="list-style-type: none"><li>• ecdh-sha2-nistp256</li></ul>	<ul style="list-style-type: none"><li>• curve25519-sha256@libssh.org</li><li>• ecdh-sha2-nistp384</li><li>• ecdh-sha2-nistp521</li><li>• diffie-hellman-group-exchange-sha256</li></ul>
Cipher	<ul style="list-style-type: none"><li>• aes256-cbc</li><li>• aes128-cbc</li><li>• chacha20-poly1305@openssh.com</li></ul>	<ul style="list-style-type: none"><li>• aes256-gcm@openssh.com</li><li>• aes128-gcm@openssh.com</li><li>• aes256-ctr</li><li>• aes128-ctr</li></ul>
HMAC		<ul style="list-style-type: none"><li>• hmac-sha2-512</li><li>• hmac-sha2-256</li></ul>

## FIPS SSH configuration

The following table lists the available options for the default FIPS SSH configuration:

**TABLE 37.** FIPS SSH CONFIGURATION OPTIONS

Configuration	Available	Selected
Cipher		<ul style="list-style-type: none"><li>• aes256-gcm</li><li>• aes128-gcm</li><li>• aes256-ctr</li><li>• aes128-ctr</li></ul>
Key Exchange Algorithms		<ul style="list-style-type: none"><li>• diffie-hellman-group-exchange-sha256</li></ul>
HMAC		<ul style="list-style-type: none"><li>• hmac-sha2-512</li><li>• hmac-sha2-256</li></ul>

## CC SSH configurations

The following table lists the available options for the default Common Criteria (CC) SSH configuration:

**TABLE 38.** CC SSH CONFIGURATION OPTIONS

Configuration	Available	Selected
Cipher	<ul style="list-style-type: none"><li>• aes256-gcm</li><li>• aes128-gcm</li><li>• aes256-ctr</li><li>• aes128-ctr</li></ul>	<ul style="list-style-type: none"><li>• aes256-cbc</li><li>• aes128-cbc</li></ul>
Key Exchange Algorithms	<ul style="list-style-type: none"><li>• diffie-hellman-group-exchange-sha256</li></ul>	<ul style="list-style-type: none"><li>• diffie-hellman-group-exchange-sha256</li></ul>
HMAC		<ul style="list-style-type: none"><li>• hmac-sha2-512</li><li>• hmac-sha2-256</li></ul>

# Maintenance Settings

- [Maintenance overview](#)
- [Software updates](#)
- [Self Diagnosis](#)
- [Export configuration](#)
- [Import a configuration](#)
- [Clear configuration](#)
- [System Storage](#)
- [Reboot](#)
- [System backup](#)

## Maintenance overview

System Manager **Maintenance** menu options contains menu items for configuring Ivanti EPMM access. The following table summarizes the tasks associated with each menu item.

**TABLE 39.** MAINTENANCE MENU ITEMS

Settings Menu	Task
Software Updates	Upgrade, configure, and manage software versions. Refer to the appendix <a href="#">Upgrading Ivanti EPMM Releases</a> for details.
Export Configuration	Export system configuration files for backup.
Import Configuration	Import backed up system configuration files.
Clear Configuration	Clear unsaved configuration settings and return to the default configuration.
System Storage	Monitor disk storage availability.
Reboot	Reboot the Ivanti server, clear the current configuration settings, and to restart all server modules.

**TABLE 39.** MAINTENANCE MENU ITEMS (CONT.)

Settings Menu	Task
System Backup	Test connectivity to the backup server, schedule daily backups, and perform an immediate backup.
Optimize Database	Optimize Ivanti EPMM database performance by cleaning up fragmentation in the database.

## Software updates

Use the **Maintenance > Software Updates** feature to upgrade, configure, and manage software versions. Refer to [Upgrading Ivanti EPMM Releases](#) for details.

## Export configuration

Use the **Maintenance > Export Configuration** feature to back up the system configuration.

### Procedure

To export the Ivanti Server configuration settings to XML format:

1. Log into System Manager.
2. Go to **Maintenance > Export Configuration**.
3. Click **Export**.

## Import a configuration

Use the **Maintenance > Import Configuration** feature to back up the system configuration.

### Procedure

To import an Ivanti Server configuration from a local XML file or FTP site:

1. Log into System Manager.
2. Go to **Maintenance > Import Configuration > Select File**.
3. Click **Choose File**.
4. Select the file.
5. Click **Import**.



## Clear configuration

Use the **Maintenance > Import Configuration** feature to clear unsaved configuration settings and return to the default configuration.

### Procedure

To clear the configuration:

1. Log into System Manager.
2. Go to **Maintenance > Clear Configuration**.
3. Click **Clear Configuration**.

## System Storage

Use the **Maintenance > System Storage** options to monitor disk storage availability. Running out of disk space can result in corrupting the Ivanti EPMM database. Therefore, this feature ensures that:

- You are aware when disk space availability is becoming too low. Once warned, you can clean up the Ivanti EPMM database and avoid database corruption.
- Ivanti EPMM services are automatically stopped when disk space availability reaches the lowest threshold, thereby avoiding database corruption when no more disk space is available.

Ivanti EPMM can send you an email when it detects that its available disk storage space has dropped below thresholds that you define. Specifically, when the available space is less than a:

- **Warning Threshold:** to receive a warning email.
- **Stop Threshold:** to receive an email and after a five minute delay, Ivanti EPMM stops its critical services if you selected that option.

When notified, you can use existing CLI commands to clean up the Ivanti EPMM database, thereby freeing up disk space. The CLI commands are:

- **dbcleanup purge\_data**
- **diskcleanup retired\_devices**

Using these commands is described in the ["Increasing available disk storage" on page 124](#) section of this chapter.



Hover over the **System Storage** bar to see a popup indicating the actual storage usage and capacity.

---

Although the Event Center system event **System storage threshold has been reached** (set in the Admin Portal's **Logs > Event Settings**) you will still receive a notification, no automatic action results from the event being triggered. Without immediate action, the possibility of running out of disk space and database corruption is more likely.

This section includes the following topics:

- ["Configuring system storage thresholds" below](#)
- ["Stopped Ivanti EPMM services" on the next page](#)
- ["Increasing available disk storage" on page 124](#)
- ["Restart Ivanti EPMM services" on page 124](#)

## Configuring system storage thresholds

Use **Maintenance > System Storage** to set the disk storage capacity thresholds and use System Manager to enable automatically stopping critical Ivanti EPMM services.

### Procedure

To configure the disk storage capacity thresholds:

1. Log into System Manager.
2. Go to **Maintenance > System Storage**.
3. Go to the System Storage options and check the box next to **Check free space capacity every**.
4. Select how many days between each check.
5. Select the time of day for each check.



**Important** The system uses GMT (Greenwich Mean Time). Select a time that is during your work hours so that you see the notification emails at a time of day when you can take actions.

---

6. Enter the email addresses for receiving the notifications. Separate email addresses with commas.

7. Select a **Warning Threshold**. For example, if this value is set to 20%, an email notification is sent when disk storage availability drops to less than 20% of disk storage capacity.
8. Select a **Stop Threshold**. For example, if this value is set to 10%, an email notification is sent when disk storage availability drops to less than 10% of the threshold:
9. Select **Stop all critical Ivanti EPMM services when stop threshold is met**.

Refer to the "[Stopped Ivanti EPMM services](#)" below table for more information.

Ivanti EPMM delays stopping the services until five minutes after the threshold is met. You cannot cancel the stop action once it is triggered.

10. Click **Save**. You will receive emails when a threshold is met.

## Example

### Warning Threshold email

```
Storage has reached a warning threshold of 50%.
```

```
Total Size : 197300M
```

```
Used Size : 92621
```

```
Available Size : 94651
```

```
Note: Cleanup the disk space using CLI commands.
```

### Stop Threshold email

```
Storage has reached a stop threshold of 45%. EPMM services will be stopped in 5 minutes, if not already stopped
```

```
Total Size : 197300M
```

```
Used Size : 137503M
```

```
Available Size : 49769M
```

```
Note: Cleanup the disk space using CLI commands. Reboot Ivanti EPMM to restart the services
```

## Stopped Ivanti EPMM services

When disk storage availability drops below the stop threshold, and you have selected the option to stop critical services, Ivanti EPMM stops are listed in the following table:

**TABLE 40.** IVANTI EPMM SERVICES STOPPED

Service stopped	Impact to stopping the service
Ivanti EPMM	<p>Stopping this service stops:</p> <ul style="list-style-type: none"><li>• Communication with devices</li><li>• Communication between Ivanti EPMM and Sentry</li><li>• Admin Portal</li><li>• User Portal</li></ul> <p>However, the following are still running:</p> <ul style="list-style-type: none"><li>• System Manager</li><li>• CLI</li></ul>
RDB Exporter	Ivanti EPMM does not send data to the Reporting Database

## Increasing available disk storage

When the warning threshold or stop threshold is reached, use CLI commands to clean up the disk storage.

### Procedure

1. Use ssh to log in to Ivanti EPMM.
2. Enter **enable** to access EXEC PRIVILEGED CLI mode.
3. Enter the "enable secret" password.
4. Enter **dbcleanup purge\_data** to clean up the database. If Ivanti EPMM services are not already stopped, this command stops them and restarts them when it finishes the clean up.
5. If Ivanti EPMM services are not already stopped, this command stops them and restarts them when it finishes the clean up.
6. Enter **diskcleanup retired\_devices** to clean up retired devices from the disk.
7. Restart Ivanti EPMM if any Ivanti EPMM services were stopped.

## Restart Ivanti EPMM services

You can use the following methods to restart Ivanti EPMM services:

- System Manager
- CLI command

## Restarting Ivanti EPMM services using System Manager

### Procedure

1. Log into System Manager.
2. Go to **Maintenance > Reboot**.
3. Click **Reboot > Yes**.

## Restarting Ivanti EPMM services using the CLI

### Procedure

1. Use ssh to log in to Ivanti EPMM.
2. Enter **enable** to access EXEC PRIVILEGED CLI mode.
3. Enter the "enable secret" password.
4. Enter **reload**.

## Reboot

Use **Maintenance > Reboot** to reboot the Ivanti server, clear the current configuration settings, and to restart all server modules.

### Procedure

1. Log into System Manager.
2. Go to **Maintenance > Reboot**.
3. Click **Reboot > Yes**.

## System backup

Use this option to testing connectivity to the backup server, scheduling daily backups, and performing an immediate backup.



An Ivanti EPMM system backup does not include the Splunk forwarder configuration within Ivanti EPMM. Therefore, after the system is restored, you must manually configure Splunk forwarder.

---

Ivanti recommends restricting access to port 22 or SSH from the internal corporate network only. This service is intended for Ivanti Standalone Sentry System Manager and must have strictly controlled access.

This section contains the following topics:

---

- ["Prerequisites for configuring system backups" below](#)
- ["Enabling backups" below](#)
- ["System backup status" on the next page](#)
- ["Configuring system backup settings" on page 129](#)
- ["System Backup Configuration group" on page 129](#)
- ["Running an immediate system backup" on page 131](#)
- ["Restore a system backup" on page 131](#)
- ["Create local backup" on page 133](#)
- ["Restore System" on page 134](#)

## Prerequisites for configuring system backups

This section lists the prerequisites for configuring system backups.

- Sufficient disk space at the destination to store the archive
- Protocol-specific requirements described in the following table:

**TABLE 41.** SYSTEM BACKUP PREREQUISITES

Protocol	Prerequisites
NFS	Port 2049 open from Ivanti EPMM to the NFS server.  The NFS option assumes that user authentication is not required for the specified server. Therefore, Ivanti recommends using IP ACLs to restrict NFS mounts to Ivanti EPMM.
SCP	Port 22 open from Ivanti EPMM to the backup location.
FTP	Port 21 open from Ivanti EPMM to the FTP server.
CIFS	Ports 137 (UDP), 138 (UDP), 139 (TCP), and 445 (TCP) open from Ivanti EPMM to the Windows share server.  SMB v2.0 through the latest version as supported by Ivanti.

## Enabling backups

### Procedure

To enable the configured backup schedule:

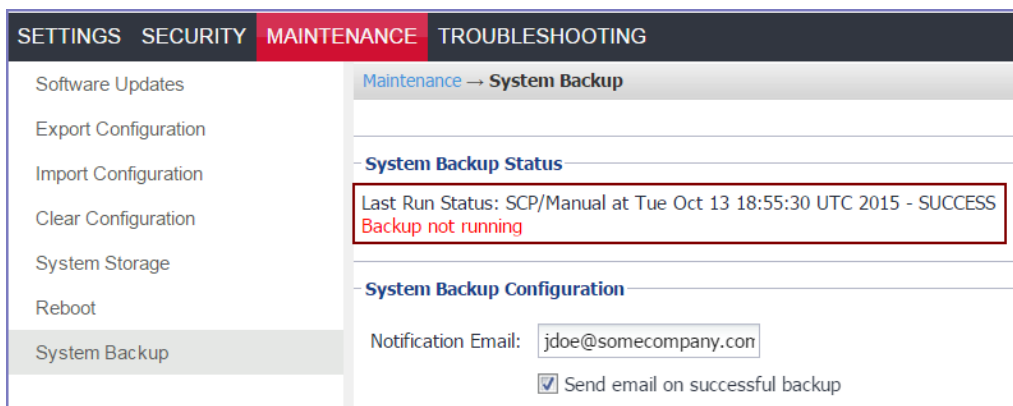
1. Log into System Manager.
2. Go to **Maintenance > System Backup**.
3. Go to the **System Backup Control** group.
4. Select **Enable** for the **System Backup** option.

## System backup status

Use the **Maintenance > System Backup Status** group to track status of the backup. Starting a backup, activates the **Backup is running** indicator in the **System Backup Status** section. When it completes, a brief status message displays the following information:

- Date and time of the backup
- Backup type (LOCAL, FTP, NFS, CIFS, or SCP)
- Whether the backup was scheduled (automatic) or run now (manual)
- Whether the backup was successful

FIGURE 1. SYSTEM BACKUP WINDOW



Ivanti EPMM executes a set of validations to verify that the backed up database is not corrupted. If any of the validations fail, the status message indicates that the backup failed. The same validations occur whenever a backup is attempted. For example, the validations occur when backing up Ivanti EPMM in a High Availability environment

## System backup email notifications

Email notifications about a successful or failed backup contain the following information:

- The time of the success or failure
- The size of the backup
- Time taken to perform the backup
- Backup type (FTP, SCP, NFS, or CIFS)
- Backup server IP address or name
- Path of backup location on the backup server
- The reason for a backup failure

Possible failure reasons given are:

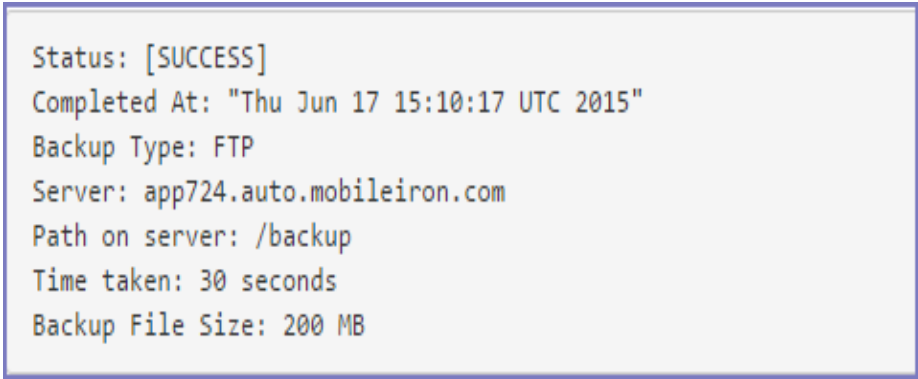
- Mount fail
- Server not available
- Authentication failure
- Not enough disk space on the server
- Not enough disk space on Ivanti EPMM
- Failed to access the directory

Use this information to take actions to ensure the success of subsequent backups. For example, if you are notified that you are out of disk space on your backup server, you can remove old files from the backup server.

### Example

The following are examples of emails for successful and failed backups:

FIGURE 2. SUCCESSFUL BACKUP EMAIL EXAMPLE



```
Status: [SUCCESS]
Completed At: "Thu Jun 17 15:10:17 UTC 2015"
Backup Type: FTP
Server: app724.auto.mobileiron.com
Path on server: /backup
Time taken: 30 seconds
Backup File Size: 200 MB
```



FIGURE 3. UNSUCCESSFUL BACKUP EMAIL EXAMPLE

```
Status: [FAILED]
Failure Reason: "Authentication Failed"
Completed At: "Thu Jun 17 15:10:17 UTC 2015"
Backup Type: FTP
Server: app724.auto.mobileiron.com
Path on server: /backup
Time taken: 4 seconds
Backup File Size: 200 MB
```

## Configuring system backup settings

Complete the following steps to configure the destination and schedule for backups:

### Procedure

1. Log into System Manager.
2. Go to **Maintenance > System Backup**.
3. Scroll to the **System Backup Configuration** group.
4. Modify the fields, as necessary. Refer to the "[System Backup Configuration group](#)" below table for more information.
5. Click **Test Connectivity**. A message displays indicating whether the connectivity test succeeded or failed.
6. Click **Save > OK** if the connectivity test succeeded. If the connectivity test failed, check the server information you entered, correct, and retry.

## System Backup Configuration group

The following table summarizes fields and descriptions in the **System Backup Configuration** group:

**TABLE 42.** SYSTEM BACKUP CONFIGURATIONS FIELDS

Fields	Description
Notification Email	Enter the email address that should receive backup/restore notifications. By default, notifications are sent only if the backup fails.
Send email on successful backup	Select this option to include notifications for success in addition to notifications for failure.

**TABLE 42.** SYSTEM BACKUP CONFIGURATIONS FIELDS (CONT.)

Fields	Description
Start time (GMT)	Select the time (GMT) at which a daily backup should occur, based on the system time set in the System Manager.
Only Backup the System Locally	<p>Select this option if you want to create a system backup that you can download onto your local machine. Creating and storing a backup locally is useful before installing an Ivanti EPMM update.</p> <p>If you select this option, the backup server fields are disabled.</p> <p>See <a href="#">"Create local backup" on page 133</a>.</p>
Backup using	<p>Select from the following protocols:</p> <ul style="list-style-type: none"> <li>• FTP</li> <li>• SCP</li> <li>• NFS</li> <li>• CIFS</li> </ul> <p>The selected protocol determines which of the following fields display.</p>
Server	<p>Enter the domain name or IP address for the server to be used.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• 10.102.0.50</li> <li>• mybackupserver.mycompany.com</li> </ul>
User	<p>Enter the user name for the account to be used.</p> <p>For CIFS, you might also need to specify the domain (e.g., MYDOMAIN\myuserid).</p>
Password	Enter the password for the account to be used.
Password Confirmation	Confirm the password for the account to be used.
Server Path	<p>Enter any additional path necessary to specify the location on the host server.</p> <p>For example, if you want to write backups to the Backups/Ivanti EPMM folder on the specified server, you would enter /Backups/Ivanti EPMM in this field.</p> <p>Be sure to include the leading forward slash (/), or the backup will fail.</p>

## Running an immediate system backup

To start an immediate system backup:

### Procedure

1. Log into System Manager.
2. Go to **Maintenance > System Backup**.
3. Scroll down to the **Run System Backup Now** section.
4. Click **Run**.

## Backup filename format

The name of the resulting file has the following format:

```
< Ivanti EPMM_FQDN>-backup-YYYY-MM-DD--HH-MM-SS.tgz
```

where < Ivanti EPMM\_FQDN> is the fully-qualified domain for Ivanti EPMM.

## Viewing backup logs

You can view system backup logs on demand and download them like other system logs,

### Procedure

1. Log into System Manager.
2. Go to **Troubleshooting > Logs**.
3. Go to the **View Module Logs** section.
4. Click the **SystemBackup** link.

## Restore a system backup

You can restore a system backup (data and configuration) or reset the existing Ivanti EPMM to the factory default state if the following requirements are met:

- The Ivanti EPMM version used to create the backup must be used to restore the backup.
- Confirm that the location of the backup file is easily accessible to ensure that the upload process does not time out. Uploading the file should complete within 15 minutes.

## Restoring a system backup

To restore a system backup:

1. Log into System Manager.
2. Go to **Maintenance > System Backup**.
3. Scroll down to the **Restore System** section.
4. Click **Choose File**.
5. Select the backup file.
6. Click **Restore**. When the process is complete, a message displays prompting you to reboot.
7. If prompted to save the configuration, click **Yes**.
8. If you chose to configure a second Ivanti EPMM instead of resetting the original, power down the original to prevent IP conflicts.
9. Select **Maintenance > Reboot > Reboot**.

## Restoring only data

Some situations call for restoring the data from a backup without restoring the system configuration. These situations include:

- confirming that expected data is included in backups
- disaster recovery

To address these situations, use the **Exclude System Configs on Restore** option.

FIGURE 4. RESTORE SYSTEM WINDOW

The screenshot shows the 'Maintenance' tab in the System Manager interface. The left sidebar lists various settings, with 'System Backup' selected. The main panel is titled 'Maintenance → System Backup' and contains the following sections:

- Configuration Fields:**
  - Two password fields labeled 'Password:' and 'Password Confirmation:', both masked with dots.
  - A 'Server Path (optional):' field containing the text '/nfs'.
  - 'Save' and 'Test Connectivity' buttons.
- Run System Backup Now:**
  - A 'Run' button.
  - A note: 'Note: The Backup File Will Be Stored Locally'.
- Restore System:**
  - A 'Restore From:' label followed by a file selection interface showing 'Choose File' and 'No file chosen'.
  - A checkbox labeled 'Exclude System Configs on Restore', which is currently unchecked and highlighted with a red rectangle.
  - A 'Restore' button.

Restoring a system in this manner does not provide a replacement Ivanti EPMM. You can use this restored system to view data or as the basis for a replacement system.

## Create local backup

You can either schedule a backup or run an immediate backup of your Ivanti EPMM instance and store it locally. Creating and storing a backup locally is useful before installing an Ivanti EPMM update.

## Configuring local backup

You can run an immediate backup or set up a scheduled backup using the follow these steps to create a local backup.

### Procedure

1. Log into System Manager.
2. Go to **Maintenance > System Backup**.
3. Go to the **System Backup Configuration** group.
4. Scroll to the **Backup Location Preferences** section.

5. Check **Only Backup the System Locally**.
6. Do one of the following actions:
  - From **Start Time (GMT)**, select an hour (GMT time) to run the backup at a specified time.
  - In **Run System Backup Now**, click **Run** to run the backup immediately.
7. Click **Save**.
8. After the backup is run, click **Download Backup** in **System Backup Status**.

## Restore System

Use a locally downloaded file on your desktop to restore the system or one that has been copied to a remote file server.



Do not revert to earlier versions of Ivanti EPMM using a snapshot after enabling mutual authentication. Doing so may necessitate re-enrolling devices.

---

To restore the system:

### Procedure

1. Log into System Manager.
2. Go to **Maintenance > System Backup**.
3. Scroll to the **Restore System** group.
4. Select **Exclude System Configs on Restore**.
5. This allows you to restore the backup to a new system without effecting the existing system. This can also be used to test a backup and restore procedure without effecting the main system. If do not select to **Exclude System Configs on Restore** the system will reboot to the IP and host configuration that was in the backup file.
6. Select **Restore** to upload your backup file and add it to the system.
7. When you are prompted reboot, go to **Maintenance > Reboot** and click **Reboot**.

## Optimize database

Use the **Maintenance > Optimize database** feature to optimize Ivanti EPMM database performance by cleaning up fragmentation in the database. Fragmentation of the Ivanti EPMM database can lead to Ivanti EPMM performance degradation. The System Manager display for optimizing the database to clean up fragmentation makes it easy for you to improve Ivanti EPMM performance.

This section includes the following topics:

- ["Optimizing the database " below](#)
- ["Optimizing the database" on the next page](#)

## Optimizing the database

Ivanti EPMM services stop when you optimizing the database. Therefore, Ivanti recommends running database optimization during a maintenance period. See ["Stopped Ivanti EPMM services" on page 123](#) for a list of all the services that are stopped when you optimize the database.

After the optimization is completed, Ivanti EPMM services are restarted.

Optimizing the database can take a long time. The duration can depend on:

- the size of the database, which depends on number of users, devices, apps, policies, and so on, in Ivanti EPMM.
- the level of fragmentation that you specify.
- the number of tables that exceed the fragmentation level you specify, and their level of fragmentation.

### Do not reboot Ivanti EPMM while database optimization is running

Rebooting while database optimization is running can result in a corrupted database. Do not reboot. If you believe that the optimization run is not ending (hung), contact Ivanti Technical Support.

### Optimize the database after deleting retired devices

You can delete retired devices in the Admin Portal in **Settings > System Settings > Users & Devices > Delete Retired Devices** or by using the Ivanti EPMM web services API. Deleting retired devices removes device records from the database. If the action deletes many retired devices, significant disk space is freed, which means a database optimization will reduce fragmentation and improve Ivanti EPMM performance.

Therefore, Ivanti recommends that if you have a large number of retired devices to delete, delete them during a maintenance period, and follow the action with database optimization.

## Optimizing the database

### Procedure

1. Log into System Manager.
2. Go to **Maintenance > Optimize database**.
3. Set **Optimize Table Fragmentation Level** to a value between 10% and 60%.

The fragmentation level indicates the percent of disk space allocated for a database table that is not in use (free table space / total table space). A higher percentage means higher fragmentation.

The screen displays all database tables with a fragmentation higher than the specified value.

Set a higher level, such as 60%, to display, and then optimize, only the most fragmented tables. Use a lower level, such as 10%, to display, and then optimize, all (or almost all) tables.

See "[Optimization tables](#)" on the next page table for details.

4. Click **Run Now** to clean up fragmentation in the displayed tables.

The display indicates:

Optimization Status :  Optimization is running...

- Do not reboot Ivanti EPMM while the optimization is running. A reboot during optimization could corrupt your database. The optimization can take many minutes, even hours. You can monitor the process by selecting **View Status Logs**.

Contact Ivanti Technical Support if the optimization does not finish.

- Running database optimization stops Ivanti EPMM services.

When the optimization completes Ivanti EPMM services are restarted.

The display updates the list of tables and their fragmentation information.



After optimizing the database, smaller tables sometimes still show a significant fragmentation level. This fragmentation level is normal. It occurs because of the small size of the table and the minimum allocation size for tables.



## Optimization tables

The following table summarizes the fragmentation options.

**TABLE 43.** FRAGMENTATION LEVEL OPTIMIZE TABLE

Tables	Information
<b>Allocated Size (MB)</b>	The total amount of disk space that is allocated to the table.
<b>Free Size (MB)</b>	The amount of the disk space allocated to the table that is not in use.
Fragment %	The percent of disk space allocated to the table that is not in use ( <b>Free Size / Allocated Size</b> ). A higher percentage means higher fragmentation.



# Troubleshooting

Troubleshooting overview .....	139
Working with logs .....	140
Network monitor .....	146
Service diagnosis .....	147
System monitor .....	148
Queue Activation .....	151
In-Memory Queue Monitor .....	151

## Troubleshooting overview

Troubleshooting menu options provide you with the opportunity to investigate possible problems with Ivanti operation. In most cases, you will use this page under the direction of Ivanti Technical Support.

The following table summarizes the tasks associated with each menu item.

**TABLE 44.** TROUBLESHOOTING MENU ITEMS

Settings Menu	Task
Logs	Enable, disable, clear, view, and export logs.
Network Monitor	Produce a TCP dump for one of the Ivanti Server physical interfaces.
Service Diagnostic	Check the health of the following services: <ul style="list-style-type: none"><li>• Support_Site</li><li>• MapQuest</li><li>• DNS</li><li>• NTP</li><li>• Email</li></ul>
System Monitor	Monitor Ivanti EPMM performance over a period of time.
Queue Activation	Performance troubleshooting with Ivanti Technical Support.
In-Memory Queue Monitor	Provides Ivanti Technical Support with information about tasks in the queue in your Ivanti EPMM memory.

## Working with logs

Use the **Troubleshooting > Logs** options to:

- Setting the log level for Stunnel and HTTPD logs
- Exported logs
- Enable debugging for Ivanti modules
- Disable debugging for Ivanti modules
- Clear logs
- View logs
- Exporting logs

### Setting the log level for Stunnel and HTTPD logs

#### Setting the Stunnel log level

In **Troubleshooting > Logs**, in the section **Stunnel/HTTPD Log Management**, you can set the log level for Stunnel. Stunnel is a library that Ivanti uses for TLS encryption. These logs are captured in the `/var/log/mi_` messages file. The default log level is **Emergency**. Typically, you do not need to change the Stunnel log level. Ivanti recommends that you contact Technical Support before changing the log level.

#### Setting the httpd log level

In **Troubleshooting > Logs**, in the section **Stunnel/HTTPD Log Management**, you can set the log level for events related to incoming HTTP/HTTPS requests. These logs are captured in the files in `/var/log/httpd/https_error_log` and `/var/log/httpd/portal_error_log`. The default log level is **Warning**. Typically, you do not need to change the httpd log level. Ivanti recommends that you contact Technical Support before changing the log level.



Changing the log level to **Debug** or **Trace** causes many events to be logged. Ivanti EPMM maintains up to 5 100MB files for each of the log files in `/var/log/httpd`. When the maximum is exceeded, Ivanti EPMM deletes the oldest file.

---

### Exported logs

The `/var/log/httpd` logs and `/var/log/elasticsearch/elasticsearch.log` are now exported to the `splunk` and `syslog` settings.

---

## Enabling debugging for Ivanti EPMM modules

You can specify which Ivanti EPMM modules you want to place in debug mode. Placing a module in debug mode causes more detailed messages to be recorded in the corresponding log.

### Procedure

1. Under **Troubleshooting > Logs**, select the check boxes for the modules you want to place in debug mode:

MICS	MobileIron Configuration Service (the service that supports System Manager)
MIFS	MobileIron File Service (the service that supports the rest of Ivanti EPMM)

2. For MIFS (MobileIron File Service), which represents the rest of Ivanti EPMM, select:
  - a. In the **MIFS Debugging** section, use the **Package** drop-down to select an area to include in the log.
  - b. Use the **Log level** drop-down to select the level of detail you want to include.
  - c. Click the + icon to add additional packages and log levels.
3. Click **Apply**.

## Disabling debugging

You can disable all debugging or you can select the modules for which you want to disable debugging.

### Disabling all debugging

To disable all debugging, which stops Ivanti EPMM from writing detailed information to all logs, click **Stop All Debugging** under **Troubleshooting > Logs**. For MIFS packages, clicking this button sets the log level to **Info** for all selected packages.

### Disabling debugging for MICS or the employee portal

#### Procedure

1. Log into System Manager.
2. Go to **Troubleshooting > Logs**.
3. Go to the **Log Management** group.

4. Clear the checkbox next to each module you want to remove from debug mode.
5. Click **Apply > OK**.

## Disabling debugging for MIFS packages

### Procedure

To disable debugging for MIFS packages under **Troubleshooting > Logs**:

1. Remove the package from the list (sets lowest level of logging)
2. Set the log level to OFF (turns off all logging for the selected package)

## Clearing logs

Clearing logs enables you to discard information for previous events, making it easier to isolate the information you need.

### Procedure

1. Log into System Manager.
2. Go to **Troubleshooting > Logs**.
3. Go to the **Log Management** group.
4. Click **Clear All Logs**.

## Log Names

The **Troubleshooting** screen enables you to view the contents of debug logs directly from the console. Debugging must be enabled. The following table lists the available logs:

**TABLE 45.** VIEWING LOGS

Log Name	Description
MICS	Ivanti Configuration Service-related log files (the service that supports System Manager).
MIFS	Ivanti File Service-related log files.
System	Ivanti EPMM status logs-related log files.
Device	Searchable device log files (search by mobile number or user).

**TABLE 45.** VIEWING LOGS (CONT.)

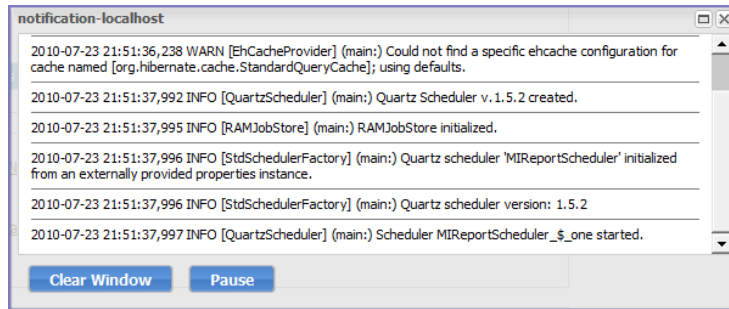
Log Name	Description
MI	Ivanti back-end system-related log files.
Catalina	Ivanti application loading status-related log files.
Catalina2	Ivanti application loading status-related log files.
SystemBackup	Ivanti System Backup process-related log files. See <a href="#">"System backup" on page 125</a> .
High Availability	HA service-related log files, if configured.
LDAP	Lightweight Directory Access Protocol (LDAP) integration-related log files.
CertActivity	Certificate activity-related log files.
CertCheckJobStatus	Certificate status-related log files.
DEP	Apple Automated Device Enrollment-related log files.
VPP	Apple volume purchase plan-related log files.
SSP	Self-service user portal-related log files.

## Viewing logs

### Procedure

1. Log into System Manager.
2. Go to **Troubleshooting > Logs**.
3. Go to **View Module Logs** section

- Click the link for the log you want to view.



The window scrolls dynamically as Ivanti EPMM adds entries to the log. The most recent log entries are at the top.

- Click **x** to close the log view.

If you close the log view window and then re-open it, the displayed window shows only log entries made since you closed the window.

## Viewing only new log entries

### Procedure

To remove existing log entries from the log view window and view only new log entries:

- Log into System Manager.
- Go to **Troubleshooting > Logs**.
- Go to **View Module Logs** section
- Click the **Clear Window** button.

## Viewing logs by device or user

### Procedure

- Log into System Manager.
- Go to **Troubleshooting > Logs**.
- Go to **View Module Logs** section
- Click the **Device** link.
- Select **User** or **Phone** to specify whether you want to view logs by user or device.



6. Enter the user name or phone number.
7. Click **View Log**.

## Exporting logs

You can upload logs directly to the default support site or a designated alternate site. The default support site is configured in **Settings > Log Upload**.

Typically, you will use the default HTTPS Server Configuration, which automatically includes the user name you entered in **Maintenance > Software Updates**. Confirm with Technical Support that the entries on this display are correct.

### Procedure

To upload logs:

1. Select **Troubleshooting > Logs**.
2. Scroll down to the **Export Logs** section.
3. Select the log to download.
4. Select a database option.

Show tech logs can include database information that some companies consider too sensitive to send to Customer Support. Therefore, you can use the **Database Options** to specify whether to include data and whether to remove potentially sensitive information from the output.

The following options are available:

- **Sanitize**: Remove sensitive information. This is the default selection. If you select the **Sanitize** option, the following data is removed:
  - email addresses
  - device tokens
  - unlock tokens
  - phone numbers
  - last locations
  - unsent alerts
  - events

- **Standard:** Sensitive information included.
  - **No Database:** All database information omitted.
5. Select **SFTP Upload**, **HTTPS Upload** or **Download** from the **Type** drop-down list, depending on the method you want to use.



For Self-service user portal (SSP) log files, **Download** is the only supported Export option.

---

6. If you received an Ivanti support ticket number associated with this export, enter it in the **Support Ticket Number** field.
7. If you selected **SFTP Upload** or **HTTPS Upload**, select the **Alternate Location** check box and configure a backup location or user authentication in case transmission to the primary server or user fails.

If you receive technical support from an Ivanti partner instead of directly from Ivanti, then you will need to obtain an alternate location from your vendor.

The following additional fields for the alternate location are displayed:

- **Host/IP or URL** (e.g., <https://support.ivanti.com>)
  - **User Name**
  - **Password**
  - **Confirm Password**
8. Click **SFTP Upload**, **HTTPS Upload** or **Download**.

## Network monitor

The Network Monitor screen lets you produce a TCP dump for one of the Ivanti Server physical interfaces. The information provided might assist in troubleshooting device connectivity problems. Click **Download** to store the results in a pcap file.

## Enabling debugging

In order to view the contents of debug logs directly from the console, you must enable debugging.

To enable debugging:

1. Log into System Manager.
2. Go to **Troubleshooting > Logs** to open the **Span Monitor Configuration** details pane.
3. Modify one or more of the fields, as necessary.  
Refer to the "[Span Monitor Configuration](#)" [below](#) table for more information.
4. Click **Download** to store the results in a pcap file.

## Span Monitor Configuration

The following table summarizes fields and descriptions in the **Span Monitor Configuration** details pane:

**TABLE 46.** SPAN MONITOR CONFIGURATION FIELDS

Option	Description
Interface	Select the physical interface for which you want to produce a tcp dump.
Filter	Not implemented.
Snap Length	Not implemented.
Max no. of Packets	Specifies the number of packets after which the capture should stop. The default value is 1000. Acceptable range of values is 1 to 1000000.

## Service diagnosis

You can use the Service Diagnosis page under Troubleshooting to check the health of the following services:

- Support\_Site
- MapQuest
- DNS
- NTP
- Email

Click the **Verify All** button to recheck all listed services, or click the **Verify** button next to a specific service to verify just that service.

## LDAP sync history

To confirm that LDAP synchronization has been performed as expected, click **LDAP Sync History**.

### Related topics

- "Managing LDAP users" in *Getting Started with Ivanti EPMM*

## System monitor

The System Manager provides the capability to monitor Ivanti EPMM performance over a period of time. Ivanti EPMM collects the performance information into log files. Ivanti Technical Support uses these files to diagnose Ivanti EPMM performance issues.

The files contain information about:

- CPU usage
- memory usage
- threads
- tomcat performance
- database performance
- mysql logs

You can download the files, or upload them to an external server that Ivanti Technical Support specifies.

To monitor Ivanti EPMM performance when working with Ivanti Technical Support, go to the System Manager to **Troubleshooting > System Monitor**.

You can run the system monitor daily and on demand. If you are experience Ivanti EPMM performance issues, collecting system monitor logs can help Ivanti Technical Support diagnose the issue.

## Running the system monitor

### Procedure

1. ["Configuring the server to upload the log files" on the next page](#) - You can skip this step if you plan to download the log files from running the system monitor to the computer on which you are running the System Manager. Only the log files from the most recent system monitor run are available.
2. ["Configuring the system monitor" on the next page](#) -

## Configuring the server to upload the log files

When you run the system monitor, you can either:

- Download the resulting log files to the computer on which you are viewing the System Manager.
- Upload the resulting log files to an SFTP or HTTPS server.

### Procedure

If you want to upload the files to an SFTP or HTTPS server, do the following:

1. Log into System Manager.
2. Go to **Settings > Log Upload**.
3. To upload system monitor logs to an HTTPS server, enter the URL of the HTTPS server.

Using an SFTP server is not supported.

4. Enter the **User Name** and **Password** for the appropriate server.

When working with Ivanti Technical Support, they will provide the credentials. If you upgraded Ivanti EPMM, the credentials you entered on **Maintenance > Software Updates** are automatically filled into this display.

5. Enter the password again in **Confirm Password**.
6. Click **Apply** for the server configuration you just entered.

## Configuring the system monitor

### Procedure

1. Log into the System Manager.
2. Go to **Troubleshooting > System Monitor**.
3. Select **On** for the **Status** field to enable the system monitor. Selecting **Off** disables the system monitor.



**Important:** When disabled, the daily system monitor runs do not occur, and you cannot select **Run Now**.

---

4. For **Iterations**, enter a value between **1** and **9999**. This number specifies how many times to collect system data. Technical Support will tell you what value to use.
5. For **Intervals (Seconds)**, enter a value between **1** and **100**. This number specifies the number of seconds between each iteration. Technical Support will tell you what value to use.
6. For **Run daily at**, select the time of day you want to run the system monitor.
7. For **Export Type**, select one of the following:
  - **Download** - The latest system monitor log files will be available for download.
  - **HTTPS Upload** - System monitor files will be uploaded to the server you specify in **Settings > Log Upload**.

Another option is SFTP Upload, but this option is not supported.

8. Click **Apply**.
9. If you want to run the system monitor immediately, click **Run Now**.

## The system monitor files

Ivanti EPMM collects the system monitor log files into an archive file:

```
system-monitor-<Ivanti EPMM host name>-<date and time>.tar.gz
```

### Example

```
system-monitor-myEPMM.mycompany.com-2016-01-19-17-31-04.tar.gz
```

The tar file contains these log files:

- miiostat.log
- mitop.log
- monitor-mysql-process-<date>.log
- monitor-threads-<date>.log
- mivmstat.log
- monitor-mysql-innodb-<date>.log
- monitor-mysql-locks-<date>.log
- tomcat-catalina.out

## Queue Activation

Use Queue Activation for performance troubleshooting with Technical Support. They can use the following display for troubleshooting if you contact them regarding performance issues on Ivanti EPMM. The new display is at **Troubleshooting > Queue Activation**.

This display provides Ivanti Technical Support information about what is running on Ivanti EPMM. The information indicates possible causes of performance issues due to high load.

To access the Queue Activation information:

1. Log into System Manager.
2. Select **Troubleshooting > Queue Activation**.
3. Click the link next to **Real-time Queue Activation Data** to display one of the following data views:
  - Real-time Data
  - Historical Data

## In-Memory Queue Monitor

This display provides Ivanti Technical Support with information about tasks in the queue in your Ivanti EPMM memory.

To use this display:

1. Log into System Manager.
2. Select **Troubleshooting > In-Memory Queue Monitor** to see the **Summary View**.

The summary table includes the following columns:

- Queue Name
  - Current Size
  - Enqueued Delta
  - Dequeued Delta
  - Enqueued Total
  - Dequeued Total
3. Click **Detailed View** to see the same details from a selected queue.

The detail table includes the following columns:

- Time Reported
- Current Size
- Enqueued Delta
- Dequeued Delta
- Enqueued Total
- Dequeued Total

4. Click a queue name from the dropdown to select a queue from the list to see its details.



# Upgrading Ivanti EPMM Releases

Upgrading overview .....	153
Upgrade planning notes .....	153
Upgrade Ivanti EPMM using System Manager .....	156
Updating Ivanti EPMM using the CLI .....	159
Ivanti EPMM OS and platform updates .....	161
Advanced: SAML .....	163

## Upgrading overview

Use the **Maintenance > Software Updates** feature to upgrade, configure, and manage software versions. The information in this chapter describes how to upgrade Ivanti EPMM releases. Ivanti EPMM software uses the term "updates" to refer to upgrading software from one release to another. It also uses the term "update" for getting the latest information or linking to 3rd party upgraded software. Because there can be slight and subtle differences between these concepts, this documentation will use the same terminology found in the System Manager UI and call-out distinctions, when necessary.

Refer to the ***Ivanti EPMM Release Notes and Upgrade Guide*** for the latest build information, available on the Ivanti Support Community site [here](#). Refer to the "Terminology" on page 5 section in Chapter 1, which provides instructions on how to access Ivanti product documentation.

## Upgrade planning notes

Upgrading software requires preparation and planning. Read this section before beginning upgrading Ivanti EPMM, for important information that will help you plan your upgrade. This section includes the following topics:

- "First-generation physical appliances" on the next page
- "Upgrade URLs" on the next page
- "Preparing the Windows Phone app" on the next page
- "Activating Apple Device Enrollment after upgrading" on page 155
- "LDAP group user and group names for IBM Domino server" on page 155
- "SMS option in Privacy policy" on page 155

## First-generation physical appliances

Upgrading is not supported for first-generation physical appliances. For information on how to determine whether you have a first-generation appliance, see <https://forums.ivanti.com/s/article/How-to-Identify-Your-MobileIron-Appliance-1498>.

## Upgrade URLs

The upgrade procedure presented in this chapter assumes you are using the default upgrade URL. If you intend to specify an alternate URL, **be sure to include the build number of the target upgrade**. Go to **Maintenance > Software Updates > software repository configuration > Default** and enter the alternate URL.

## Preparing the Windows Phone app

The following information applies to Windows Phone apps that have been rebranded for distribution by Ivanti partners only.

If you have Windows Phone devices currently enrolled, complete the following steps after the upgrade to ensure that the Windows Phone app is silently deployed to those devices.

### Procedure

1. Log into the Ivanti EPMM Admin Portal.
2. Go to **Apps > App Distribution Library**.
3. Go to the **Select Platform** list.
4. Select **Windows Phone**.
5. Select the entry for the Windows Phone app.
6. Select **Actions > Apply to Label**.
7. Select the Windows Phone label.
8. Click **Apply > OK**.

## Activating Apple Device Enrollment after upgrading

Apple Device Enrollment lets you purchase Apple devices in bulk and register them with both Apple and your Ivanti EPMM easily and quickly. To use Apple Device Enrollment, after upgrading from Ivanti VSP 6.0 or earlier, **you must assign the role for administering Apple Device Enrollment accounts to one or more Super Administrators or Global Administrators (administrators assigned to the Global space).**

### Procedure

To assign administration of Apple Device Enrollment accounts to a Super Administrator or Global Administrator:

1. Log into the Ivanti EPMM Admin Portal.
2. Go to **Admin > Admins**.
3. Select a **Global** or **Super Administrator**.
4. Select **Actions > Edit Roles**.
5. Select **Manage device enrollment (iOS only)**.
6. Click **Save**.

## LDAP group user and group names for IBM Domino server

A dynamic label problem exists after upgrading from an Ivanti EPMM version prior to 7.0, if:

- An LDAP group name is the same as an LDAP username in a different LDAP group
- An LDAP user with the duplicate name is assigned to a dynamic label

If these conditions exist, the LDAP user with the duplicate name is no longer associated with the dynamic label after the upgrade. To resolve this issue, either rename the user before upgrading, or associate the LDAP user with the dynamic label again after the upgrade.

## SMS option in Privacy policy

Upgrading from releases prior to Ivanti EPMM 7.0 resets the **SMS** option in the Privacy policy to **None**. If you had previously configured the **SMS** option to **Sync Content**, edit the Privacy policy after the upgrade and reset the **SMS** option to **Sync Content**.

## Upgrade Ivanti EPMM using System Manager

When you upgrade Ivanti EPMM it is important to properly set up the environment and all necessary components. Read and complete each section before upgrading Ivanti EPMM using System Manager.

- ["Content development preparation" below](#)
- ["VM requirements" below](#)
- ["Backup availability" on the next page](#)
- ["Updating Ivanti EPMM" on the next page](#)

### Content development preparation

Software downloads are supported through both:

- Ivanti support page
- a content development network (CDN)

A CDN can improve software download speed. When you request an upgrade without specifying a URL, the download proceeds using a CDN by default. If the upgrade cannot proceed via CDN, then the upgrade automatically redirects to Ivanti support page.

Make the following preparations to support upgrade via CDN:

- Firewall rules must include HTTPS outbound to support-cdn.mobileiron.com (the CDN URL).
- We recommend allowing all outbound HTTPS traffic in your firewall rules because the location of data hosted on a CDN can change.
- An outbound connection to the Internet is necessary to ensure reliability.

### VM requirements

Before upgrading a virtual Ivanti EPMM, confirm that your VM instance meets requirements. See the latest *On-Premise Installation Guide for Ivanti EPMM and Enterprise Connector* for these requirements.

## Backup availability

It is always prudent to create backups prior to upgrading. You have different options for performing a backup:

- Use the **Backup and Restore** feature in System Manager.
- If Professional Services has implemented backups for your system, make sure you have a recent successful backup.
- If you are using a virtual Ivanti EPMM, consider creating a .vmdk backup.

## Updating Ivanti EPMM

### Procedure

TLS authentication is mandatory for users to upgrade the software. The user must enable the Mutual authentication check box on the Ivanti EPMM admin portal under Settings > Security > Certificate Authentication. To upgrade Ivanti EPMM software using the System Manager:

1. Log into System Manager.
2. Go to **Maintenance > Software Updates** to display the **Software Updates** options.
3. Go to the **Software repository configuration** group.
4. Enter the credentials assigned by Ivanti Support.
5. Click **Apply > OK**.
6. Click **Check Updates** to show a list of the available updates.
7. Select the update you want.
8. Click **Download Now** if you want to download the update now and complete the installation at a later time.
9. Refresh the screen and click **Check Updates**.


After the download is complete, the status for the update changes to **Downloaded**.

10. Click **Validate** to validate the database and select one of the following options:

**Validate Database structure (schema)** to verify that the existing database has the right database structure to proceed with upgrade. If the validation fails, do not proceed with the upgrade and contact Ivanti Support.

**Validate the Database structure and Data** to copy the database to a temporary database to run the validation then click **Yes** to stop EPMM services, (required for validation).

---


 Validating the database with data can take up to 4 hours, depending on the database size.

---

The **Validation Status** include the following options:

- **Not Running**
- **Validation Running**
- **Validation Failed**
- **Validation is Successful**

---

 This step is option, but highly recommended. It alerts you to any problems that can happen during the upgrade process and can avoid the upgrade if the Validate DB returns errors. When the DB validations has no errors, then you can proceed with upgrading the environment.

---

11. Refresh the screen and click **Check Updates**.

After the software update has been staged for installation, the status for the update changes to **Reboot to Install**. You can now install the update by rebooting the system. If the status of an update is not Reboot to Install, rebooting the system will not install the update.

12. Select **Maintenance > Reboot** to reboot Ivanti EPMM. To successfully install the update, you must reboot after the status is **Reboot to install**.
13. Click **Stage for Install** when you are ready to install. If you have already downloaded the selected update, the system stages the update for installation. If you did not previously download the selected update, it is downloaded and staged for installation.
14. Click **Yes** to agree to the End User License Agreement and proceed further.
15. Refresh the screen and click **Check Updates**.
16. Continue with "[Verifying the upgrade is complete](#)" on the next page.

## Verifying the upgrade is complete

To verify that the upgrade is complete:

Ivanti recommends to allow HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for EPMM server management and must have strictly controlled access.

1. Go to the Ivanti EPMM System Manager:

`https://<FQDN>:8443/mics`

2. Select **Maintenance > Software Updates**.
3. Confirm that the current version is correct.



**Important!** Under no circumstances should you restart the upgrade. Contact Ivanti Technical Support if you need assistance. Once this upgrade procedure is complete, it may take up to 5 minutes for Ivanti Client apps to display in the **App Catalog** page.

---

## Viewing upgrade status

Go to the following URL to see the progress of an upgrade: <https://FQDN:8443/upgrade/status>.

## Updating Ivanti EPMM using the CLI

Use the Ivanti EPMM CLI as an **alternate** way to upgrade Ivanti EPMM. When you upgrade Ivanti EPMM it is important to properly set up the environment and all necessary components. Read and complete each section before upgrading Ivanti EPMM using the CLI:

- ["Configuring your update repo" below](#)
- ["Initiating the upgrade" on the next page](#)
- ["Rebooting Ivanti EPMM" on page 161](#)

## Configuring your update repo

### Procedure

To configure your update repo:

---

1. Log into the CLI using the administrator account you created during installation.
2. Enter the following command to switch to EXEC Privileged mode: **enable**
3. Enter the password for enabling the EXEC Privileged mode.

The command line prompt changes: **#**

4. Enter the following command to enable CONFIG mode: **configure terminal**
5. Enter the following command to specify the URL and credentials for the repo:

**software repository https://support.mobileiron.com/mi/vsp/<version and build number>/mobileiron-<version and build number> <username> <password>**

### Example

**software repository https://support.mobileiron.com/mi/vsp/9.0.0.0-96/mobileiron-9.0.0.0-96 <username> <password>**

In the above command, *<username>* and *<password>* are your company's download/documentation credentials as provided by Ivanti Technical Support.



For the URL of the Ivanti EPMM release to which you want to upgrade, see "Ivanti EPMM upgrade URL" in the release notes for that Ivanti EPMM release.

---

## Initiating the upgrade

Under no circumstances should you restart the upgrade. Contact Ivanti Technical Support if you need assistance.

### Procedure

1. Enter the following command to exit CONFIG mode: **end**
2. To list the updates available, enter the following command: **software checkupdate**
3. Confirm that there are no errors displayed.
4. Enter the following command to download the latest available updates: **software update**



## Rebooting Ivanti EPMM

### Procedure

1. After all the listed updates are installed, enter the following command to reload the appliance: **reload**

The following message displays: System configuration may have been modified. **Save? [yes/no]**

2. Enter **no**.

The following message displays: **Proceed with reload? [yes/no]**

3. Enter **yes**. The reboot could take up to 15 minutes to complete.

The following error might display on the console and should be resolved after you complete the remaining upgrade steps:

```
modprobe: FATAL: Could not load /lib/modules/2.6.18.c15/modules.dcp: No such file
or directory
```

4. To confirm that the upgrade is complete, make sure you can log into the Admin Portal:  
**https://<FQDN>/mifs.**

## Ivanti EPMM OS and platform updates

Ivanti EPMM can update several types of data without requiring an Ivanti EPMM upgrade:

- device operating system and version (iOS 9.0 or Android 6.0, for example)
- platform type (Android Knox phone or Apple iPad, for example)

For example, when Apple makes a new iOS version available, you do not need to upgrade Ivanti EPMM.

You can choose whether these updates occur automatically or require administrative action. The default value is automatic update. The benefit is you can update your Ivanti instance to support updated devices, operating systems and versions without upgrading Ivanti EPMM. You can also choose between:

- ["Automatic data update " below](#)
- ["Manual data update " on the next page](#)

### Automatic data update

You can change data update control between automatic update and administrator control. The default setting is automatic update.

To use automatic data updates, you must make sure a port is open for the App Gateway. To open a port for App Gateway, see the *On-Premise Installation Guide for Ivanti EPMM and Enterprise Connector* for details. The table containing the entry for App Gateway (appgw.ivanti.com) is in the section "Internet/Outside Rules."

### Procedure

If you are using manual updates, but decide to resume automatic updates:

1. In System Manager, go to **Maintenance > Software Updates**.
2. In **Device and Platform Updates**, check **Auto update device and platform support**.
3. Click **Save**.

If you are using automatic updates, but need to use manual updates instead:

1. In System Manager, go to **Maintenance > Software Updates**.
2. In **Device and Platform Updates**, clear **Auto update device and platform support**.
3. Click **Save**.

## Manual data update

If your organization has blocked the App Gateway, you will need to manually update device and platform information:

### Procedure

To set up manual operating system and device data updates:

1. Log into System Manager.
2. Go to **Maintenance > Software Updates**.
3. Scroll down to the **Device and Platform Updates** options.

4. Go to the end of the paragraph in **Manually update OS, Device and other Ivanti EPMM data** and click the word **here** to display a website containing the following information:
  - **Upload File:** a link to download the file containing the update information
  - **Checksum:** checksum for the file
  - **Time Stamp:** time stamp for the file
5. Go to the release of the package you want to download.
6. Click **Download Update File** to download the file with the update information.
7. Return to System Manager > Maintenance > Software Updates > Device and Platform Updates.
8. Go to the **Upload File** option and click **Choose File**.
9. Navigate to the file you downloaded and click **Open**.
10. Copy the checksum from the website and paste it in **Checksum** field in System Manager.
11. Copy the time stamp from the website and paste it in **Time Stamp** field in System Manager.
12. Click **Update**.
13. In **Device and Platform Updates** under **Update available**, click **Update Now** to immediately update Ivanti EPMM with the new information from the file.

If you do not update Ivanti EPMM immediately, Ivanti EPMM is updated either within:

- 15 minutes after Ivanti EPMM is restarted
- within 24 hours of the next App Gateway update

## Advanced: SAML

Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP).

Ivanti recommends to allow HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for EPMM server management and must have strictly controlled access.

This section contains the following topics:


- ["Configuring SAML/IdP support" below](#)
- ["Deactivating or deleting the IdP metadata file" on the next page](#)

Use this feature to allow local administrator users to use single-sign on for the Admin Portal and self-service user portal. This feature also allows administrators to automatically redirect authentication for the Admin Portal and the user portal to your external IdP.

Enabling SAML restarts Ivanti EPMM, which disrupts services until the configuration is complete. Therefore, access to the Admin Portal and self-service user portal is not available until after the SAML/IdP configuration is successfully completed. Furthermore, username/password authentication and certificate authentication to the Admin Portal and the self-service user portal will be disabled.

SAML is not supported on the System Manager portal. However, when SAML is enabled, local users can authenticate to the System Manager with a user ID and password, but not with certificate authentication.

---

 If you set up SAML after setting the Admin Portal to run on port 8443, automatic redirection to the Admin Portal and to the self-service user portal will succeed. If you set up SAML after setting the Admin Portal to 443 redirection will not succeed until you reconfigure the Admin Portal to run on port 8443.

Ivanti recommends to allow HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for EPMM server management and must have strictly controlled access.

---

You must reconfigure SAML using the System Manager if both of the following are true:


- You upgraded to this version of Ivanti EPMM from a version of Ivanti EPMM prior to 10.0.0.0.
- You had configured SAML using the command line on Ivanti EPMM. Note that configuring SAML from the command line is not supported from Ivanti EPMM 9.7 through the current Ivanti EPMM release.

Contact Ivanti Technical Support if you have authentication failures in this scenario.

## Configuring SAML/IdP support

This topic describes how to configure SAML over IdP. For more details, refer to Microsoft documentation.

---

 Once set up for SAML on iReg or DEP devices, you will not be able to disable SAML from the System Manager. You must first de-select the "SAML-based registration" field in Ivanti EPMM's Device Registration page before you can disable the IdP SAML connection in the System Manager.

---

### Before you begin

- Create at least one SAML user, with associated permissions.
- Sign up with an external IdP.
- Be able to export the metadata file from the IdP.

### Procedure

1. Log into the System Manager Portal.
2. Go to **Security > Advanced > SAML**.
3. Click the box to **Enable** SAML.
4. Read the warning message and click **Yes** to restart Ivanti EPMM and turn on SAML. This can take a few minutes. The **Configuration Status** changes from **Restarting Tomcat...** to **In Progress**, followed by **Completed**.
5. Click **Download** to download the XML metadata file from Ivanti EPMM that was created as part of the Ivanti EPMM restart process.
6. Save this file locally.
7. After downloading and saving the metadata from Ivanti EPMM, upload the Ivanti EPMM metadata files to your IdP:
  - a. Export those metadata files from your idP, and upload them to Ivanti EPMM.
  - b. Click **Done > OK**.
  - c. Verify the IdP hostname/URL and modify it, if necessary. System Manager extracts the hostname or URL from the IdP metadata file and auto-populates these fields.
8. Click **Apply**.



If you do not complete configuring SAML, reboot Ivanti EPMM by selecting **Maintenance > Reboot > Reboot** in the System Manager.

---

## Deactivating or deleting the IdP metadata file

This topic describes how to deactivate or delete the SAML/IdP option.

### Procedure

1. Log into the System Manager Portal.
2. Go to **Security > Advanced > SAML**.
3. Click the box to **Disable** SAML to deactivate SAML or click **Delete** to delete the SAML file.

There is no option to delete the IdP metadata file - they upload a new one which replaces the previous one.