ivanti

On-Premise Installation Guide for Ivanti EPMM and Enterprise Connector 11.4.0.0 - 11.12.0.0

Revised: August 2024

Revision history

For the complete revision history, see the online version of this document.

Contents

Pre-deployment tasks

This document provides you with all the information required to install Ivanti EPMM starting with the pre-deployment tasks described in this chapter. This chapter includes the following topics:

- "New customer resources" below
- "New customer checklists" below
- "Deployment components" on page 10
- "Internal corporate network rules" on page 11
- "External and Internet rules" on page 13
- "Additional firewall rules" on page 19
- "Enroll in the Apple certificate and iDEP programs" on page 23
- "Purchase third-party trusted certificates" on page 27
- "Preparing for Android Enterprise device support" on page 28
- "Preparing for Windows device support" on page 29

New customer resources

The following resources for new customers are available online. Some of these links will change to the Ivanti website.

- Deployment Toolkit
- Basics Doc 1 (Develop Your Project Plan)
- Make the Most Out of MobileIron University (MIU)
- How to Open a Support Case
- Software Download

New customer checklists

New customer checklist can be used as a guideline for deploying your Ivanti EPMM system. New customers receive the following checklists and are reproduced here for your convenience:

- Use "Customer contact details" below to provide contact information for employees who will be involved in the engagement.

- Complete these forms to allow Ivanti, Inc and their partners to adequately size and scope your deployment environment for Ivanti EPMM and Sentry:
  - "Technical/network environment" on the next page
  - "Email infrastructure environment" on page 8
  - "Employees and devices" on page 8
  - "Ivanti EPMM product functionality" on page 9
  - "Ivanti EPMM application and control" on page 10

Customer contact details

TABLE 1. CUSTOMER CONTACT DETAILS

Role	Contact Information	
Primary customer contact (Project Manager)	**Name**:	
	Telephone:	
	Email:	
	Location:	
Primary technical contact (Ivanti EPMM administrator)	**Name**:	
	Telephone:	
	Email:	
	Location:	
Primary security contact	**Name**:	
	Telephone:	
	Email:	
	Location:	
Primary networking/firewall team contact	**Name**:	
	Telephone:	
	Email:	
	Location:	

TABLE 1. CUSTOMER CONTACT DETAILS (CONT.)

Role	Contact Information	
Primary application team contact	**Name**:	
	Telephone:	
	Email:	
	Location:	
Other technical contact(s)	**Name**:	
	Telephone:	
	Email:	
	Location:	
Executive sponsor	**Name**:	
	Telephone:	
	Email:	
	Location:	

Technical/network environment

TABLE 2. TECHNICAL/NETWORK ENVIRONMENT DETAILS

Item	Question	Response
1	Will you be deploying physical hardware or virtual appliances?	
2	Is this a fresh install, or a re-use of a POC environment or system previously installed?	
3	What type of load balancing and/or redundancy requirements do you have for your Ivanti EPMM platform?	
4	Do you have any special network requirements around your DMZ environment with regard to firmware rules, communication protocols, or integration restrictions?	

TABLE 2. TECHNICAL/NETWORK ENVIRONMENT DETAILS (CONT.)

Item	Question	Response
5	What is your Active Directory/LDAP environment? Is it accessible from the DMZ for user authentication?	
6	Are you using a single, multiple, or federated domain?	
7	Do you have an internal or hosted certificate infrastructure, and if so, which one (i.e. Microsoft with SCEP/NDES, Synmantec Web Services, OpenTrust)?	

Email infrastructure environment

TABLE 3. EMAIL INFRASTRUCTURE ENVIRONMENT DETAILS

Item	Question	Response
1	What type of email system do you use (i.e. Exchange, Office 365, Google Mail)?	
2	Is the email infrastructure distributed and/or have redundancy?	
3	How many unique domains do you support that are in scope for this engagement?	
4	Do you plan on using email attachment control?	
5	Do you plan on using Kerberos Authentication?	

Employees and devices

TABLE 4. EMPLOYEES AND DEVICES DETAILS

Item	Question	Response
1	How many total employees do you have?	
2	How many total devices are in scope for this current engagement?	

TABLE 4. EMPLOYEES AND DEVICES DETAILS (CONT.)

Item	Question	Response
3	Do you plan to support employee-owned devices, corporate-owned devices, or both?	
4	How many devices do you plan to have under Ivanti EPMM management within 6 months?	
5	How many devices do you plan to have under Ivanti EPMM management within 6 months?	
6	Estimate the devices in the deployment scope by OS type and by geographic region (see worksheet, below).	

Device Type	Region	Android	iOS	Windows Phone	Windows 10	OSX	Other
Employee and Corporate Owned Devices	**North America**						
	Europe						
	APJ						

Ivanti EPMM product functionality

TABLE 5. IVANTI EPMM PRODUCT FUNCTIONALITY DETAILS

Item	Question	Response
1	What are the top 3 business objectives you would like to address with Ivanti EPMM?	
2	What type of device registration and provisioning do you plan to implement (i.e self-registration, by invitation)?	
3	What Ivanti EPMM platform products are in the current scope for the project deployment (i.e. Ivanti Web@Work, Ivanti Docs@Work, Ivanti AppConnect, Ivanti Tunnel)?	
4	What Ivanti EPMM platform products are	

TABLE 5. IVANTI EPMM PRODUCT FUNCTIONALITY DETAILS (CONT.)

Item	Question	Response
	going to be used long term (i.e. Ivanti Web@Work, Ivanti Docs@Work, Ivanti AppConnect, Ivanti Tunnel)?	
5	Do you intend to deploy WiFi or VPN configurations?	
6	Do you intend to use shared devices or kiosk devices?	

Ivanti EPMM application and control

TABLE 6. IVANTI EPMM APPLICATION AND CONTROL INFORMATION

Item	Question	Response
1	Do you intend to deploy and manage apps?	
2	Will you be developing internally-developed apps?	
3	Will you deploy an Ivanti AppConnect-enabled app (internally developed) or Ivanti AppConnect Partner apps?	
4	Will you be leveraging Apple's DEP Program?	

Deployment components

Installing the Ivanti AppConnect solution includes installation of:

- Ivanti AppConnect
- Ivanti Sentry (optional)

Ivanti AppConnect provides the core functionality of the solution, while **Ivanti Sentry** provides either integration with ActiveSync email services or app tunneling services. The Ivanti Sentry is available in two configurations: **Standalone** and **Integrated** (email services only). The following diagram shows Standalone Ivanti Sentry. (Refer to the ***Standalone Ivanti Sentry Guide*** for details about Standalone Ivanti Sentry.)

For Firewall rules see:

Internal corporate network rules

The following table outlines the firewall rules required for internal corporate network access for:

- **Ivanti EPMM Appliance** (physical or virtual) - All ports (except UDP) should be bi-directional to allow information / data exchange between systems.
- **Ivanti Sentry Appliance** (physical or virtual, ActiveSync / Ivanti Tunnel) - Ivanti Sentry must be able to resolve the Ivanti EPMM hostname (via DNS lookup) or a hostfile entry must be added.

- 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.

- 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.

Ivanti EPMM Appliance and the Ivanti Sentry Appliance items communicate with each other.

TABLE 7. INTERNAL CORPORATE NETWORK RULES

Requirement	Description	Port
Traffic from Internal Corporate Network to .Ivanti EPMM Ivanti EPMM is in the DMZ		
Ivanti EPMM administrator access (System Manager)	Open HTTPS 8443 from the corporate network to the Ivanti EPMM appliance	HTTPS 8443
Ivanti EPMM administrator access	Open HTTPS 443 and SSH 22 from the corporate network to the Ivanti EPMM appliance	HTTPS 443, SSH 22
Ivanti EPMM Enterprise Connector (Optional LDAP Proxy)	Open HTTPS 443 from Enterprise Connector to Ivanti EPMM	HTTPS 443
Ivanti EPMM Reporting Database (Optional)	Ensure that HTTPS 7443 from the Reporting Database to Ivanti EPMM is open. It is open by default.	HTTPS 7443

TABLE 7. INTERNAL CORPORATE NETWORK RULES (CONT.)

Requirement	Description	Port
Self-service user portal	Open HTTPS 443 from the corporate network to the Ivanti EPMM appliance	HTTPS 443
Traffic from Ivanti EPMM to Internal Corporate Network Ivanti EPMM is in the DMZ		
LDAP / Active Directory	LDAP User Lookup and Authentication	TCP 636 (secure) -or- TCP 389
SMTP Relay for SMS and Email Notifications	Open TCP 25 (if not in DMZ) and define the SMTP relay server	TCP 25
DNS Lookup Open	Open UDP 53 (if not in DMZ) and define DNS server(s) ⓘ TCP is needed in case of large DNS Queries	UDP 53
NTP Time Synchronization Service	Open UDP 123 (if not in DMZ) and define NTP server(s)	UDP 123
Certificate / SCEP Server	SCEP Proxy Configuration	HTTP 443
Ivanti EPMM access to Ivanti Sentry	Open HTTPS 9090 (primary access) and HTTPS 443 (view of Ivanti Sentry certificate) to the Ivanti Sentry appliance	HTTPS 9090 and HTTPS 443
Sentry access to Ivanti EPMM	Open HTTPS 8443 to the Ivanti EPMM appliance (HTTPS 8443 is the default, but HTTPS 443 is also supported.)	HTTPS 8443
Traffic from Internal Corporate Network to Standalone Sentry Standalone Sentry is in the DMZ		
Ivanti EPMM administrator access	Open HTTPS 8443 from the corporate network to Ivanti Sentry(System Manager access)	HTTPS 8443
Ivanti EPMM administrator access	Open SSH 22 from the corporate network to Ivanti Sentry	SSH 22
Traffic from Standalone Sentry to Internal Corporate Network Standalone Sentry is in the DMZ		
CIFS-based Content Server	Open TCP 445 if using Ivanti Docs@Work with CIFS-based content	TCP 445

TABLE 7. INTERNAL CORPORATE NETWORK RULES (CONT.)

Requirement	Description	Port
	servers	
Certificate / SCEP Server	SCEP Server/CA Access (for CRL verification only)	HTTP 80 or HTTPS 443
App Server for AppTunnel	Open HTTP 80 or HTTPS 443 to the app/content server if configuring this Ivanti Sentry for AppTunnel	HTTP 80 or HTTPS 443 (typically)
Exchange ActiveSync	Open HTTP 80 or HTTPS 443 to the ActiveSync server if configuring this Ivanti Sentry for email service	HTTP 80 or HTTPS 443
DNS Lookup	Open UDP 53 (if not in DMZ) and define DNS server(s)	UDP 53
NTP Time Synchronization	Open UDP 123 (if not in DMZ) and define NTP server(s)	UDP 123
LDAP / Active Directory	Open TCP/UDP 389 Kerberos LDAP ping (optional for Kerberos-constrained delegation)	TCP/UDP 389
SMTP Relay for Sentry Console Email Notifications	Open TCP 25 (if not in DMZ) and define SMTP relay server	TCP 25
Kerberos Server	Open TCP 88 (for Kerberos-constrained delegation)	TCP 88

Related topics

- For firewall rules required for Internal rules/outside rules, see "External and Internet rules" below.
- For additional firewall rules, see "Additional firewall rules" on page 19.

External and Internet rules

The following table outlines the firewall rules required for external and internet access for:

- **Ivanti EPMM Appliance** (physical or virtual)

  > All ports (except UDP) should be 'bi-directional' to allow information / data exchange between systems.

- **Sentry Appliance** (physical or virtual, ActiveSync / AppTunnel)

> ℹ️ The Sentry must be able to resolve the Ivanti EPMM hostname (via DNS lookup) or a hostfile entry must be added.

- **Access**

Ivanti EPMM Appliance and the Sentry Appliance items communicate with each other.

TABLE 8. EXTERNAL AND INTERNET RULES

Requirement	Description	Port
Traffic from Internet/Outside of Ivanti EPMM		
Ivanti EPMM is in the DMZ		
iOS end-user devices	Open HTTPS 443 for iOS device access to the Ivanti EPMM to support MDM. If you are not using iOS MDM, then this port is not required.	HTTPS 443
End-user devices	Open HTTPS 443 from the internet to the Ivanti EPMM appliance (for client provisioning traffic) ℹ️ Using HTTPS 443 for provisioning requires signed certificates.	HTTPS 443 (evals only)
End-user devices	Open TCP 9997 from the internet to the Ivanti EPMM appliance (for TLS secured client sync traffic)	TCP 9997
MTD Threat Management Console	Open port 8883 inbound from MTD Threat Management Console to Ivanti EPMM.	Port 8883
Traffic from Ivanti EPMM to Internet/Outside		
Ivanti EPMM is in the DMZ		
Access	access-na1.mobileiron.com access-eu1.mobileiron.com	HTTPS 443
Android Enterprise	https://accounts.google.com/o/oauth2/token https://www.googleapis.com/androidenterprise	HTTPS 443

TABLE 8. EXTERNAL AND INTERNET RULES (CONT.)

Requirement	Description	Port
Ivanti EPMM Gateway and Apple APNS (HTTPS)	• **support.mobileiron.com**: For software update repository and upload of Showtech log, open access to these IP addresses: ◦ 52.53.85.126 ◦ 54.151.9.59 Ivanti recommends that you also open the following addresses, which will be used for future cloud deployment of the Application Gateway services: ◦ 54.176.117.219 ◦ 54.176.235.82 ◦ 54.193.230.188 ◦ 54.241.222.178 ◦ 54.241.114.195 ◦ 54.177.110.251 ◦ 50.18.43.125	HTTPS 443

TABLE 8. EXTERNAL AND INTERNET RULES (CONT.)

Requirement	Description	Port

	• Open HTTPS 443 (for location/number lookup data, in-app registration, APNS/FCM/GCM messaging, licensing, and support for sending SMS) to:
	
	   ◦ **coresms.mobileiron.com**
	
	   ◦ **coreapns.mobileiron.com**
	
	   ◦ **api.push.apple.com**
	
	   ◦ **coregcm.mobileiron.com**
	
	   ◦ **corefcm.mobileiron.com**
	     (current address: 199.127.90.0/23)
	
	   ◦ **appgw.mobileiron.com**
	     (current address: 199.127.90.0/23)
	
	Action required if you use Application Gateway (appgw.mobileiron.com) with explicit firewall rules: Due to scheduled Ivanti network maintenance, you must append these IP addresses to your existing firewall rules by December 16, 2022, to ensure no disruption of services:
	
	   ◦ 34.227.203.115
	
	   ◦ 34.231.78.119
	
	   ◦ 35.168.168.163
	
	   ◦ 18.207.62.107
	
	   ◦ 18.209.150.213
	
	   ◦ 23.21.143.22
	
	Note: Allow traffic to both the current and new IP addresses prior to December 16, 2022, until further notice. You will receive a customer communication email with more information about the maintenance window when it is confirmed.
	
	Note: See also: Urgent Ivanti Endpoint Manager Mobile Gateway Update.	

TABLE 8. EXTERNAL AND INTERNET RULES (CONT.)

Requirement	Description	Port
	• **a.mobileiron.net** for anonymized statistics collection. As the IP range for CDN sites (for example: supportcdn.mobileiron.com) may change from time to time, whitelist the domain name instead of the IP in the firewall if there is an option to do so. Otherwise, use support.mobileiron.com to download the updates instead of supportcdn.mobileiron.com. • **api.push.apple.com** to use APNSv2.	
Apple APNS and MDM Services	Open ports are 2195, 2197 (TCP) between Ivanti EPMM and Apple's APNS network (17.0.0.0/8) for support of APNS for iOS devices. If you are not using iOS MDM, then this port is not required. • TCP 2195: gateway.push.apple.com • TCP 2197: api.push.apple.com (optional, alternative for HTTPS 443)	HTTPS 443 TCP 2195, 2197
iOS VPP and Windows notification / check-ins	Open HTTPS 443 for the following access: **https://vpp.itunes.apple.com** (Known to be redirected to: www.apple.com, securemetrix.apple.com) ***.wns.windows.com, *.notify.windows.com**	HTTPS 443
iTunes, Maps/Location, Windows 10, Windows 8.1 RT/Pro Apps	Open HTTPS 443 or HTTP 80 for the following access: • **itunes.apple.com, *.phobos.apple.com,** and ***.mzstatic.com** for performing iTunes App Store lookups. • **https://storeedgefd.dsx.mp.microsoft.com** for Windows 10 app store lookups. • **http://marketplaceedgeservice.windowsphone.com**, **http://cdn.marketplaceimages.windowsphone.com** for performing Windows 8.1 store lookups,Windows 8.1 store search, app images and services. • **https://api.mqcdn.com** for locating devices (IP addresses vary. Perform an nslookup to determine the necessary IP addresses.)	HTTPS 443 HTTP 80

TABLE 8. EXTERNAL AND INTERNET RULES (CONT.)

Requirement	Description	Port
	• **http://store-images.microsoft.com/image/apps** **http://developer.mapquest.com** **http://store-images.s-microsoft.com/image/apps** for downloading Windows apps and graphics	
Google	Administrators must whitelist the following six IP addresses to ensure that end users can still get messages when Google migrates from Google Cloud Messaging (GMC) to Firebase Cloud Messaging (FCM): 18.207.169.70 34.206.49.117 52.20.247.99 52.22.230.26 52.45.189.15 107.22.86.228	
Traffic from Internet/Outside to Standalone Sentry Standalone Sentry is in the DMZ		
End user devices to access email via Sentry or to Access backend resources via AppTunnel or Tunnel	Open HTTPS 443 or HTTP 80 from the internet for ActiveSync client traffic or open HTTPS 443 for AppTunnel or Tunnel traffic ⓘ For the Sentry Appliance (physical or virtual ActiveSync/AppTunnel), the Sentry must be able to resolve Ivanti EPMM hostname (via DNS lookup) or a hostfile entry must be added.	HTTPS 443 or HTTP 80
Traffic from Standalone Sentry to Internet/Outside Standalone Sentry is in the DMZ		
Ivanti EPMM software upgrades	**support.mobileiron.com** (199.127.90.0/23) for software update repository and SFTP upload of showtech log ⓘ For the Sentry Appliance (physical or virtual ActiveSync/AppTunnel), the Sentry must be able to resolve Ivanti EPMM hostname (via DNS lookup) or a hostfile entry must be added.	HTTPS 443

Related topics

- For firewall rules required for the internal corporate network, see "Internal corporate network rules" on page 11.
- For additional firewall rules, see "Additional firewall rules" below.

Additional firewall rules

The following table outlines additional firewall rules from the internal corporate network to the Internet.

- Organizations with local network-connected Wi-Fi must mirror the external firewall port configuration on their local DMZ firewall in order for Wi-Fi-connected devices to register and function day to day.

- Ivanti Sentry does not support connection pooling via load balancer. Turn off your load balancer's connection pooling before deploying.

TABLE 9. ADDITIONAL FIREWALL RULES

Requirement	Description	Port
iOS Features	**For Apple Activation Lock support,** open HTTPS 443 to: **https://deviceservices-external.apple.com.** **For Apple DEP support,** open HTTPS 443 to: **https://mdmenrollment.apple.com**. These ports are not required if not using iOS MDM.	HTTPS 443
iOS (Wi-Fi Only) Devices	Open TCP 5223 to open 17.0.0.0/8 and allow iOS devices using corporate Wi-Fi to access the Apple APNS service. If you are not using iOS MDM, then this port is not required. **For devices on closed networks:** • **ax.init.itunes.apple.com**: Current file-size limit for downloading apps over the cellular network. • **ocsp.apple.com**: Status of the distribution certificate used to sign the provisioning profile.	TCP 5223
Android devices	**To allow access to Google's FCM or GCM service:** open TCP ports 5228, 5229, and 5230. GCM typically only uses TCP 5228, but it sometimes uses TCP 5229 and TCP 5230. GCM does not provide specific IPs, so you should allow your firewall to accept outgoing connections to all IP addresses contained in the IP blocks listed in Google's ASN of 15169. For older devices, consider open HTTPS 443, as well.	TCP 5228 TCP 5229 TCP 5230 HTTPS 443

TABLE 9. ADDITIONAL FIREWALL RULES (CONT.)

Requirement	Description	Port
	For Android Enterprise: • https://www.googleapis.com/androidenterprise • https://accounts.google.com/o/oauth2/token **For Help@Work for Android and iOS:** In general, TeamViewer will always work if Internet access is possible. As an alternative to HTTP 80, HTTPS 443 is also checked. It is also possible to open only TCP 5938 (required for mobile connections).	
Ivanti Docs@Work License Server	Open HTTPS 443 to the following URLs to allow access to the Ivanti Docs@Work license server: • https://api.polariskit.com **Note**: This section only applies to corporate fire-wall rules. It does apply to Ivanti EPMM connections.	HTTPS 443
AppConfig Community Repository	Open port 443 (HTTPS) to the following URLs to allow access to the Ivanti Docs@Work license server: • https://api.appthority.com/applications/bulk_query (Appthority) • https://api.mqcdn.com/sdk/mapquest-js/v1.0.0/mapquest.css (for the find my phone mapping and other options) • pki-ws.symauth.com (SymantecManagedPKI) • https://onestore.microsoft.com (BusinessStorePortal(BSP)) • https://bspmts.mp.microsoft.com/V1 (BusinessStorePortal(BSP)) • https://mobility.threatpulse.com:9443 (BlueCoat) • https://login.microsoftonline.com/{tenant_id}/oauth2/authorize (MicrosoftGraph) • https://eu-api.samsungknox.com (Samsung E-FOTA) • https://has.spserv.microsoft.com/HealthAttestation/ ValidateHealthCertificate/v1 (Windows device attestation) • https://webapi.teamviewer.com/api/v1/ (AndroidHelp@Work) • https://system.globalsign.com/cr/ws/GasOrderService (GlobalSign)	HTTPS 443

TABLE 9. ADDITIONAL FIREWALL RULES (CONT.)

Requirement	Description	Port
	• https://appconfig.cdn.mobileiron.com (iOSManagedAppConfigcommunity) • https://graph.windows.net/%s/devices/deviceId_%s?api-version=1.6 (Azureactivedirectory)	

AppConfig Community Repository outbound firewall port setting

Ivanti EPMM requires outbound firewall access on TCP port 443 to https://appconfig.cdn.mobileiron.com/com.example.OneTouchConfiguration/current/appconfig.xml for the Managed App Configuration UI to render properly.

TABLE 10. ADDITIONAL OUTBOUND ACCESS LINKS

Purpose	Host connection
Android Help@Work	https://webapi.teamviewer.com/api/v1/
Appthority	https://api.appthority.com/applications/bulk_query
Azure active directory	https://graph.windows.net/%s/devices/deviceId_%s?api-version=1.6
BlueCoat	https://mobility.threatpulse.com:9443
Business Store Portal (BSP)	https://onestore.microsoft.com
Business Store Portal (BSP)	https://bspmts.mp.microsoft.com/V1
For the Find My Phone mapping and other options	https://api.mqcdn.com/sdk/mapquest-js/v1.0.0/mapquest.css
GlobalSign	https://system.globalsign.com/cr/ws/GasOrderService
iOS Managed AppConfig community	https://appconfig.cdn.mobileiron.com
Microsoft Graph	https://login.microsoftonline.com/{tenant_id}/oauth2/authorize
Samsung E-FOTA	https://eu-api.samsungknox.com
SymantecManagedPKI	pki-ws.symauth.com
Windows device attestation	https://has.spserv.microsoft.com/HealthAttestation/ValidateHealthCertificate/v1

Related topics

- For firewall rules required for the internal corporate network, see "Internal corporate network rules" on page 11.
- For firewall rules required for Internal rules/outside rules, see "External and Internet rules" on page 13.

Enroll in the Apple certificate and iDEP programs

Managing iOS devices using Mobile Device Management (MDM) requires a certificate from Apple. Ivanti EPMM uses Apple's enhanced MDM certificate infrastructure to streamline the process of acquiring and uploading an MDM certificate. You can now complete the following tasks from a single screen within the Admin Portal:

- Generate a Certificate Signing Request (CSR)
- Upload the CSR
- Access the Apple Push Certificates Portal to request a certificate
- Upload the MDM certificate

If you already have an MDM certificate, but have not uploaded it, you can upload it from the same screen.

- If the Apple MDM certificate is created with a personal Apple ID, control of the certificate is retained by the user. While administrators cannot control the certificate, they can revoke it.
- We recommend the account and credentials used to create the MDM certificate be documented and stored in a secure location as this information will be required to generate a new MDM certificate when the existing certificate expires.
- If you are configuring Ivanti EPMM to support only MAM-only devices, skip these steps. For more information, see "Managing apps on MAM-only devices" in the *Ivanti Apps@Work Guide*.

Go to the following topics if you intend to do or have one of the following scenarios:

- "Develop and distribute in-house apps" below
- "Requesting an MDM certificate" below
- "Uploading an MDM certificate" on the next page

Develop and distribute in-house apps

If you intend to develop in-house apps for distribution, then you still need to participate in Apple's iDEP program. The enhanced MDM certificate infrastructure does not eliminate this requirement.

Requesting an MDM certificate

You can request a mobile device management (MDM) certificate from Apple.

> **ⓘ** Make sure that appgw.mobileiron.com is reachable from Ivanti EPMM.

Procedure

1. From the Ivanti EPMM Admin Portal, select **Settings > System Settings > iOS > MDM**.

2. Select the **Enable MDM Profile** option.

3. Click **Install MDM Certificate** to open the **MDM Certificate Generation** window.

4. Click **I want to create a new MDM certificate**.

5. Click **Download Certificate Signing Request**.

6. Click the **Apple Push Certificates Portal** link to start the process of requesting the MDM certificate.

7. When you receive the certificate, click **Upload MDM Certificate** to open the **Upload MDM Certificate** window.

8. Click **Browse** to select the MDM certificate.

9. Click **Upload Certificate**.

- Securely store, in an escrow-like account accessible to more than one individual, the username and credentials used to register with Apple.
- Make a note of the date when the MDM certificate expires and set a reminder to renew the certificate before it expires to avoid service outage.
- You have the option to create an alert which will notify you if the MDM certificate is revoked.

Uploading an MDM certificate

If you have already requested and received your MDM certificate from Apple, you can upload the certificate using the following steps:

Procedure

1. Log into the Admin Portal.

2. Select **Settings > System Settings > iOS > MDM**.

3. Select the **Enable MDM Profile** option to open the **MDM Certificate Generation** window.

4. Select **I already have an MDM Certificate, and want to upload it**.

5. Note: If you already had a MDM certificate installed, you will see warning dialog. Click **OK**.

6. Click **Upload MDM Certificate** to open the **Upload MDM Certificate** window.

7. Click **Browse** to select the MDM certificate.

8. Click **Upload Certificate**.

Preparing for Android Enterprise device support

This section describes the minimum network requirements for Android Enterprise devices. Android devices generally do not require you to open inbound ports on the firewall in order to function correctly. However, there are a number of outbound connections that administrators need to be aware of when setting up their network environments for Android Enterprise devices.

The list of network changes provided in the following table is not exhaustive and may change. It covers known endpoints for current and past versions of enterprise management APIs and GMS apps.

> ℹ In addition to the ports listed in the following table, Android Enterprise devices require access to Ivanti EPMM.

The following table lists the requirements for Android Enterprise devices.

TABLE 11. REQUIREMENTS FOR ANDROID ENTERPRISE DEVICES

Destination Host	Ports	Purpose
play.google.com android.com google-analytics.com googleusercontent.com gstatic.com *.gvt1.com *ggpht.com dl.google.com android.clients.google.com	TCP/443 TCP, UDP/5228-5230	Google Play and updates (APKs, app logos, etc.) gstatic.com, googleusercontent.com -- contains User Generated Content (for example, app icons in the store) *.gvt1.com, *.ggpht, dl.google.com,android.clients.google.com -- Download apps and updates, PlayStore APIs
*googleapis.com	TCP/443	Ivanti EPMM Unified Endpoint Management (UEM)/Google APIs/PlayStore APIs
accounts.google.com	TCP/443	Authentication

TABLE 11. REQUIREMENTS FOR ANDROID ENTERPRISE DEVICES (CONT.)

Destination Host	Ports	Purpose
gcm-http.googleapis.com gcm-xmpp.googleapis.com android.googleapis.com	TCP/443, 5228-5230, 5235, 5236	Google Cloud Messaging (for example, UEM Console <-> DPC communication, like pushing configs)
fcm.googleapis.com fcm-xmpp.googleapis.com	TCP/443, 5228-5230	Firebase Cloud Messaging (for example, Find My Device, UEM Console <-> DPC communication, like pushing configs)
pki.google.com clients1.google.com	TCP/443	Certificate Revocation
clients[2...6].google.com	TCP/443	Domains shared by various Google backend services such as crash reporting, Chrome Bookmark Sync, time sync (tlsdate), and many others

Google does not provide specific IPs, so you should allow your firewall to accept outgoing connections to *all* IP addresses contained in the IP blocks listed in Google's ASN of 15169 listed here https://bgp.he.net/AS15169#_prefixes.

Note that IPs of Google peers and edge nodes are not listed in the AS15169 blocks. See peering.google.com for more information about Google's Edge Network.

> See "External and Internet rules" on page 13 for firewall rules required for external and internet access for Ivanti EPMM appliances and Ivanti Sentry appliances.

Purchase third-party trusted certificates

Ivanti, Inc recommends using third-party certificates as follows:

- trusted TLS/SSL certificates for Ivanti EPMM and Standalone Ivanti Sentry.

  - Ivanti EPMM Portal HTTPS: External hostname of Ivanti EPMM server.

    Allows a client (such as a browser or app) to trust Ivanti EPMM over ports 443 and 8443. You must use a publicly trusted certificate from a well-known Certificate Authority if you are using mutual authentication.

    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.

  - Ivanti Sentry: External hostname of Ivanti Sentry server. Multiple sentries behind a load balancer will use the same external certificate.

    Allows a device to trust the Standalone Ivanti Sentry.

- trusted TLS/SSL certificates for device enrollment

  - iOS Enrollment: External hostname of Ivanti EPMM server. In most cases, the certificate will be the same as the Ivanti EPMM Portal HTTPS certificate.

    Ivanti EPMM uses this identity certificate to sign the Apple MDM configurations that it sends to iOS and macOS devices.

  - Client TLS: External hostname of Ivanti EPMM, often the same as the Ivanti EPMM Portal HTTPS certificate.

    Allows Ivanti Mobile@Work for iOS and Android to trust Ivanti EPMM over port 9997 or port 443.

- Obtain these certificates in advance to ensure appropriate lead time.

- Typically the Portal HTTPS, iOS Enrollment, and Client TLS certificates are the same certificate. However, you can use different certificates. We recommend using separate certificates for different use cases.

Related topics

"Certificates you configure on the *Ivanti EPMM System Manager Guide*" in the *Ivanti EPMM System Manager Guide*.

Preparing for Android Enterprise device support

This section describes the minimum network requirements for Android Enterprise devices. Android devices generally do not require you to open inbound ports on the firewall in order to function correctly. However, there are a number of outbound connections that administrators need to be aware of when setting up their network environments for Android Enterprise devices.

The list of network changes provided in the following table is not exhaustive and may change. It covers known endpoints for current and past versions of enterprise management APIs and GMS apps.

> ℹ️ In addition to the ports listed in the following table, Android Enterprise devices require access to Ivanti EPMM.

The following table lists the requirements for Android Enterprise devices.

TABLE 12. REQUIREMENTS FOR ANDROID ENTERPRISE DEVICES

Destination Host	Ports	Purpose
play.google.com android.com google-analytics.com googleusercontent.com gstatic.com *.gvt1.com *ggpht.com dl.google.com android.clients.google.com	TCP/443 TCP, UDP/5228-5230	Google Play and updates (APKs, app logos, etc.) gstatic.com, googleusercontent.com -- contains User Generated Content (for example, app icons in the store) *.gvt1.com, *.ggpht, dl.google.com,android.clients.google.com -- Download apps and updates, PlayStore APIs
*googleapis.com	TCP/443	Ivanti EPMM Unified Endpoint Management (UEM)/Google APIs/PlayStore APIs
accounts.google.com	TCP/443	Authentication
gcm-http.googleapis.com gcm-xmpp.googleapis.com android.googleapis.com	TCP/443, 5228-5230, 5235, 5236	Google Cloud Messaging (for example, UEM Console <-> DPC communication, like pushing configs)
fcm.googleapis.com fcm-xmpp.googleapis.com	TCP/443, 5228-5230	Firebase Cloud Messaging (for example, Find My Device, UEM Console <-> DPC communication, like pushing configs)
pki.google.com	TCP/443	Certificate Revocation

TABLE 12. REQUIREMENTS FOR ANDROID ENTERPRISE DEVICES (CONT.)

Destination Host	Ports	Purpose
clients1.google.com		
clients[2...6].google.com	TCP/443	Domains shared by various Google backend services such as crash reporting, Chrome Bookmark Sync, time sync (tlsdate), and many others

Google does not provide specific IPs, so you should allow your firewall to accept outgoing connections to *all* IP addresses contained in the IP blocks listed in Google's ASN of 15169 listed here https://bgp.he.net/AS15169#_prefixes.

Note that IPs of Google peers and edge nodes are not listed in the AS15169 blocks. See peering.google.com for more information about Google's Edge Network.

> ℹ See "External and Internet rules" on page 13 for firewall rules required for external and internet access for Ivanti EPMM appliances and Ivanti Sentry appliances.

Preparing for Windows device support

This section describes how to prepare for Windows device support, (Windows Mobile 8.1 and Window 10 devices). This section includes:

- "Windows device support requirements " below
- "Setting up autodiscovery" on the next page
- "Connecting to the Windows Store" on page 31

Windows device support requirements

The following table lists the requirements for Windows device support.

TABLE 13. REQUIREMENTS FOR WINDOWS DEVICES

Requirements	Required	Optional
Publicly trusted certificate for registration (Portal certificate)	X	
Autodiscovery: If autodiscovery is not set up, the registration process requires the device user to enter the Ivanti Sentry server address, that is, the FQDN for your Ivanti Sentry		X
DNS A record	X	
SAN: Includes portal and **enterpriseenrollment.** *YourCompanyDomainName.com*	X	

Setting up autodiscovery

Autodiscovery allows Windows devices to seamlessly register with Ivanti EPMM and Ivanti Sentry. The following set up is required for using autodiscovery with Windows devices:

- "Create DNS A record" below to point to Ivanti EPMM and Ivanti Sentry.
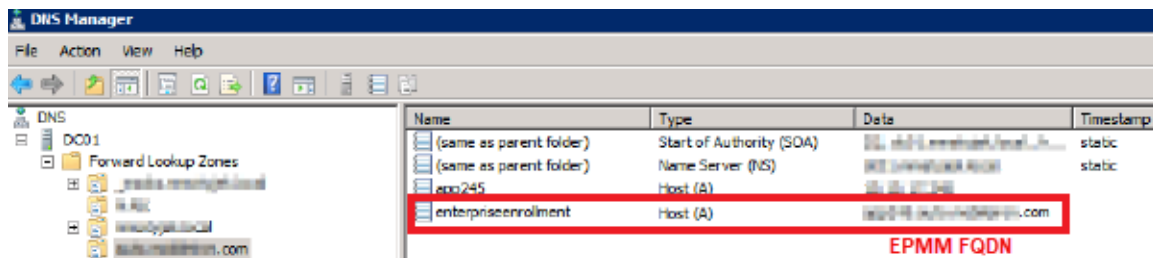- "Obtain a TLS/SSL SAN certificate" on the next page from a trusted Certificate Authority (CA)

Create DNS A record

Create a DNS A record that refers DNS requests for **enterpriseenrollment.*YourCompanyDomainName*.com** to the Ivanti EPMM IP address.

> ℹ️ *YourCompanyDomainName* must match the domain of the email addresses used for registering with Ivanti EPMM.

FIGURE 1. ENTERPRISE ENROLLMENT

Obtain a TLS/SSL SAN certificate

For Windows devices, a Subject Alternative Name (SAN) TLS/SSL certificate from a trusted Certificate Authority (CA), such as Verisign or GoDaddy, is required. If you use a self-signed (localCA) certificate, device enrollment will fail.

- The TLS/SSL certificate provides trusted and secured connection without certificate warnings.
- A SAN certificate, also known as a multi-domain certificate or a unified communication certificate, is valid for two or more hosts. The SAN certificate must cover the Ivanti EPMM hostname and enterpriseenrollment.***YourCompany-Domain name***.com.

Connecting to the Windows Store

You can set up recommended apps that device users can download from the Ivanti Apps@Work app. For Windows devices, your firewall must allow connections to the following hosts:

TABLE 14. WINDOWS HOST CONNECTIONS YOUR FIREWALL MUST ALLOW

Purpose	Host connection
Windows 10 app store search	https://storeedgefd.dsx.mp.microsoft.com
Windows 10 VPN for Cisco AnyConnect	https://www.windowsphone.com
Windows Phone 8 App store detail URL	http://marketplaceedgeservice.windowsphone.com
Windows Phone 8 app store icon URL	http://cdn.marketplaceimages.windowsphone.com

ⓘ   See "External and Internet rules" on page 13 for which ports to open.

Installing Ivanti EPMM

This chapter includes the following sections:

> When you install Ivanti EPMM on either a virtual machine or physical appliance, by default Ivanti EPMM supports only Mobile Application Management (MAM), not Mobile Device Management (MDM) on iOS devices. To enable MDM for iOS devices, after your installation is complete, see "Managing Mobile Device Management (MDM) certificates for iOS and macOS" in *Getting Started with Ivanti EPMM.*

Ivanti EPMM appliance setup

If you are installing a physical appliance, you will need to configure the system either with a standard VGA monitor and keyboard, or via the serial console. To access to the serial console, you can use a PC or remote console system. Use Putty or HyperTerminal if you are using a PC.

To set up console access:

1. Connect a console cable to the appropriate port on the back of the appliance.
2. Connect a serial cable to a PC or remote console system.

Hardware appliances

The following table describes which appliances are supported on Ivanti EPMM and Enterprise Connector .

TABLE 15. APPLIANCES SUPPORTED BY IVANTI EPMM AND ENTERPRISE CONNECTOR

Product	Supported	Compatible
Ivanti EPMM	M2250, M2600, M2700	N/A

Maximum number of supported devices

The following table summarizes the maximum number of supported devices on each Ivanti EPMM appliance.

TABLE 16. DEVICE CAPACITY FOR IVANTI EPMM APPLIANCES

Model	Maximum Number of Devices	Testing Standard
M2600, M2700	200,000	The maximum number of supported devices, for each appliance, is based on a rate of 1 device registration per second. This maximum number of supported devices will change, depending on individual use cases and work load for each appliance.
M2250	60,000	IPv4 is supported.

Virtual Ivanti EPMM requirements

If you are installing a virtual Ivanti EPMM, you need to ensure that the minimum requirements are met. This section lists the requirements for Ivanti EPMM.

Other topics in this section include:

- "Storage devices" on page 37
- "Minimum memory and CPU for Ivanti EPMM (VMware, Hyper-V)" on page 38
- "Minimum specification (VMware, Hyper-V)" on page 38
- "Gather required Ivanti EPMM information" on page 39

The following table lists the virtual Ivanti EPMM requirements. (Alternative memory and CPU configurations are not covered by the Ivanti EPMM product warranty.)

TABLE 17. VIRTUAL IVANTI EPMM REQUIREMENTS

Components	Requirements
Hard drive	Ivanti recommends configuring only one hard drive on the virtual machine. System performance is directly related to hard disk drive performance. We recommend using only high-performance tier I storage products.
Backup VMware	Ivanti recommends taking periodic .vmdk backups of your Virtual Appliance as part of your system maintenance. Use VMware VCB or another VMware-supported backup system. A backup of the full virtual disk is recommended; VMware snapshots are not sufficient.

VMware	• Download link or package (ISO) from Ivanti Support here: https://support.ivanti.com/support/CDL.html
	
	• VMware ESXi 6.5, 6.7, 7.0
	
	• 64-bit VM
	
	• Network adapter:
	   ◦ E1000
	   ◦ VMXNET 3
	
	• VM OS Type:
	
	   ◦ CentOS 7.4 (64-bit)
	
	• CPU Settings:
	   ◦ Shares: Normal
	   ◦ Reservation: Match the specification in "Minimum memory and CPU for Ivanti EPMM (VMware, Hyper-V)" on page 38.
	   ◦ Limit: Unlimited (maximum assigned)

TABLE 17. VIRTUAL IVANTI EPMM REQUIREMENTS (CONT.)

Components	Requirements
	- Memory Settings: - Shares: Normal - Reservation: Match the specification in "Minimum memory and CPU for Ivanti EPMM (VMware, Hyper-V)" on page 38. - Alternate reservation: 50% of the specification in "Minimum memory and CPU for Ivanti EPMM (VMware, Hyper-V)" on page 38.* *** The alternative memory configuration is not covered by the Ivanti product warranty.** - Limit: Unlimited (maximum assigned) - MAC address: Static allocation - Boot from BIOS firmware We currently support the LSI logic SAS or Parallel SCSI controllers; para-virtualized controllers are not supported. ⓘ Alternative memory and CPU configurations are not covered by the Ivanti EPMM product warranty
Hyper-V	- Download link or package (ISO) from Ivanti Support here: https://support.ivanti.com/support/CDL.html - Microsoft Hyper-V Server 2008, Microsoft Hyper-V Server 2008 R2, or Microsoft Hyper-V Server 2012, Microsoft Hyper-V Server 2012 R2, Microsoft Hyper-V Server 2016, Microsoft Hyper-V Server 2019 - Hyper-V MAC Address: Static allocation - Generation 1 VM - Boot from BIOS firmware - Minimum 4 GB RAM Microsoft Hyper-V Server 2008 requires a legacy network adapter. ⓘ New features in Microsoft Hyper-V Server 2016 (discrete device assignment, shielded virtual machines, disk encryption, secure boot, etc.) are not supported.

TABLE 17. VIRTUAL IVANTI EPMM REQUIREMENTS (CONT.)

Components	Requirements

Kernel-based Virtual Machine (KVM)	• Download link or package (ISO) from Ivanti Support here: https://support.ivanti.com/support/CDL.html
	
	• Minimum configuration of host machine:
	  ◦ Quad Ivanti EPMM CPU, 2 GHz clock rate
	  ◦ 16 GB RAM
	  ◦ 8 GB guest memory
	
	   ⓘ Performance data for different CPU and RAM and memory configurations is not available.
	
	• **Supported KVM version**: QEMU emulator version 2.0.0 (Debian 2.0.0+dfsg-2ubuntu1.22)
	Ivanti EPMM supports only this KVM version, but later versions are compatible.
	
	• **Supported Virtual Machine Manager version**: 0.9.5
	Ivanti EPMM supports only this Virtual Machine Manager version, but later versions are compatible.*
	
	• **Supported Linux distribution**: Ubuntu Server version 14.4 (3.19.0-25-generic #26~14.04.1-Ubuntu SMP)
	Ivanti EPMM supports only this Linux distribution, but other Linux distributions are compatible.*
	
	• In the **Virtual Machine Manager**, when creating a new virtual machine, select **Generic** for the OS type and the Version.

TABLE 17. VIRTUAL IVANTI EPMM REQUIREMENTS (CONT.)

Components	Requirements
	• **Boot from BIOS firmware**. For more information about setting up KVM, see: https://help.ubuntu.com/community/KVM. * Ivanti defines **supported** and **compatible** as follows: ○ **Supported product versions:** The functionality of the product and version with currently supported releases was systematically tested as part of the current release and, therefore, will be supported. ○ **Compatible product versions:** The functionality of the product and version with currently supported releases has not been systematically tested as part of the current release, and therefore not supported. Based on previous testing (if applicable), the product and version is expected to function with currently supported releases. ℹ For more information about setting up a Kernel-based Virtual Machine (KVM), see **https://help.ubuntu.com/community/KVM**.

Storage devices

The following table lists the requirements for storage devices.

TABLE 18. STORAGE DEVICE REQUIREMENTS

Operation	Min IOPS	Bandwidth	90% Operations < xxx mS
Random Read	400	3 MBps	10 mS
Random Write	900*	15 MBps	4 mS

Storage device notes

- Ivanti recommends configuring only one storage device per virtual machine.
- RAID controller may have to be specifically configured in order to achieve high Random Write IOPS (For example: Disk Cache: **Enabled**, Default Write: **Write Back with BBU**).
- System performance is directly related to storage device performance. We recommend using only high-performance tier 1 storage products.

Minimum memory and CPU for Ivanti EPMM (VMware, Hyper-V)

The following table captures the minimum memory and CPU recommendations based on devices tested by Ivanti.

> ℹ️ These recommendations are based on internal tests performed by Ivanti and may vary with real-time deployments. The performance might change depending on an individual use case and work load for an environment.
> If you observe performance issues in your environment, Ivanti recommends using the next set of values.

TABLE 19. MEMORY AND CPU FOR IVANTI EPMM (VMWARE, HYPER-V)

Maximum Devices	Memory	Virtual CPU / Min Clock Rate	Total Available Storage Capacity	Min Storage IOPS (Random Read)	Min Storage IOPS (Random Write)
< 5,000	8 GB RAM*	Qty 2 / 2.13 GHz processors**	80 to 250GB SAS	400	1000
< 20,000	16 GB RAM*	Qty 4 / 2.13 GHz processors**	250 GB SAS	400	1000
< 50,000	32 GB RAM*	Qty 8 / 2.13 GHz processors**	500 GB SAS	400	1000
< 100,000	64 GB RAM*	Qty 16 / 2.13 GHz processors**	1TB SAS	400	1000

* Resource allocation - no ballooning allowed

** Resource allocation - no sharing allowed with other VMs

Minimum specification (VMware, Hyper-V)

The following minimum specification does not include significant use of the app store or Ivanti Docs@Work.

TABLE 20. MINIMUM SPECIFICATIONS

Maximum devices	Memory	Virtual CPUs	Disk
< 500	8 GB RAM*	1 x 2.13GHz processors**	80 to 250GB SAS
Random Write	900*	15 MBps	4 mS

*Guaranteed resource allocation - no ballooning allowed

**Guaranteed resource allocation - no sharing allowed with other VMs

Gather required Ivanti EPMM information

Use the following table to gather and record Ivanti EPMM information before installation.

TABLE 21. IVANTI EPMM INFORMATION

Item	Description	Values
Licensing agreement information	The company name, contact person name, and contact person email address for the end-user licensing agreement.	
Ivanti EPMM Server IP Address	Static IP address for portal access.	
External Hostname	Fully-qualified domain name for Ivanti EPMM. **Do not use an internal hostname. Managed devices must be able to access Ivanti EPMM from the Internet.**	
"enable secret" password	The Ivanti EPMM password to be defined for enabling access to Privileged and Configuration modes.	
Administrator User Name	The user name to define for the Ivanti EPMM Administrator. **Do not use root or ha_admin.**	
Administrator Password	The Ivanti EPMM Administrator password must contain the following elements: • At least 8 characters. • At least 1 alphabetic character. • At least 1 numeric character. • Cannot have 4 or more repeating characters. • Cannot be the same as the user ID. • May contain Unicode characters, except for CLI access. ⓘ Users cannot change a password more than once during a 24 hour period.	

TABLE 21. IVANTI EPMM INFORMATION (CONT.)

Item	Description	Values
Physical Interface	The physical interface to use on the appliance. Enter a or b. You can configure additional physical interfaces later using the System Manager.	
IP Address Netmask	The IP address and netmask of the physical network interface.	
Default Gateway	The IP address of the router used to forward traffic to destinations outside of the local network or subnet.	
Name Server 1, 2, 3	The IP address of a network name server (i.e., DNS server). You must specify at least one name server.	
Remote Shell via SSH?	Specifies whether you want to configure remote shell access via SSH.	
NTP Server 1, 2, 3	Specifies the IP address of an optional reliable time source. We recommend specifying an NTP server. If you do not, you will have the opportunity to set the system clock and date.	

Installing VMware ISO

Complete the following steps to install Ivanti EPMM using VMware ISO distribution.

Procedure

1. If you have not done so already, create a VM that meets the specifications recommended by Ivanti. See "Virtual Ivanti EPMM requirements" on page 33 for recommended specifications.

2. Make sure the MAC address is set to: Static allocation.

3. Place the ISO distribution in an existing vSphere datastore.

4. In the vSphere Client, select the **Edit Settings** option for the VM you created.

5. Select Datastore ISO File.

6. Click **Browse** to select the Ivanti EPMM ISO distribution.

7. Make sure the **Connected** and **Connect at power on** options in the **Virtual Machine Properties** window are selected.

8. Select **Host Device**.

9. Click **OK**.

10. Power on the VM.
   The VM automatically installs and reloads after a few minutes, and the installation program starts. See for the next steps.
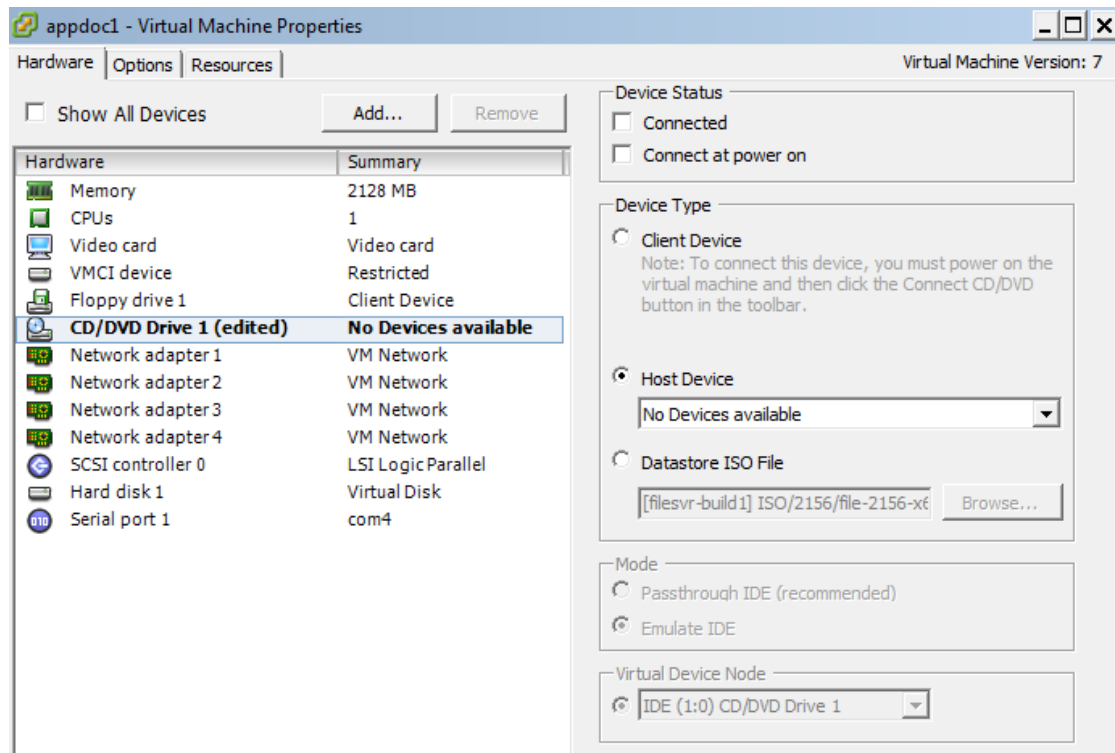
Installing Hyper-V ISO

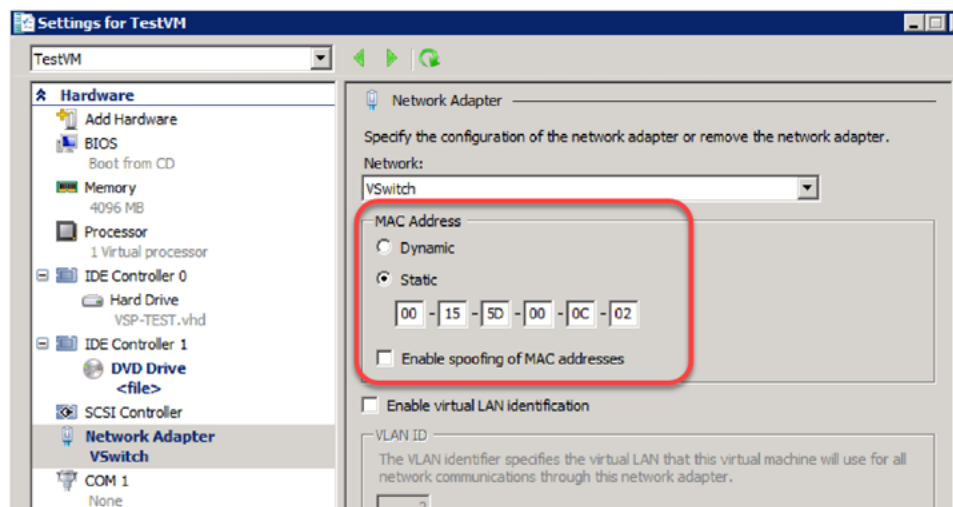Complete the following steps to install Ivanti EPMM using Hyper-V ISO distribution.

Procedure

1. If you have not done so already, create a VM that meets specifications recommended by Ivanti. See "Virtual Ivanti EPMM requirements" on page 33 for recommended specifications.

> Verify static and dynamic allocation of RAM. For example, if the suggested RAM is 8 GB as per Ivanti EPMM guidelines, then set the RAM memory to a guaranteed allocation of 8 GB.

2. Place the ISO distribution in an existing datastore.

3. In Hyper-V Manager, right-click the name of the VM you created, then click **Settings**.

4. To install from an ISO image, select **Image File**, click **Browse**.

5. From the **Open** dialog box, select the ISO file in the datastore.

6. Set Hyper-V MAC setting from **Dynamic** to **Static.** To change the Hyper-V MAC settings, click on **VM settings > Network adapter.** For **MAC Address**, select **Static**.

> At the very first boot, static MAC address will be shown as all 0 or empty. If you do not know the MAC address, select MAC Address as 'Dynamic' to assign on its own. After ISO installation, you can stop the VM and set it to static with the assigned/fetched MAC address.

7. Click **Apply**, then **OK**.

8. Start the VM.

The VM automatically installs and reloads after a few minutes, and the installation program starts. See for the next steps.

Installing Ivanti EPMM ISO onto an appliance

You can install a Ivanti EPMM ISO onto an appliance using a DVD or USB flash drive, depending on the appliance. This section describes the preparation and installation process.

- "Preparing a USB flash drive for installation" below
-
-

Preparing a USB flash drive for installation

The M2250, M2600, and M2700 appliances do not have a DVD drive. Therefore, use of a DVD with these appliances is not supported. Installing the Ivanti EPMM ISO on these appliances is done from a USB flash drive.

> ⓘ USB flash drives are only supported on M2250, M2600, and M2700 appliances.
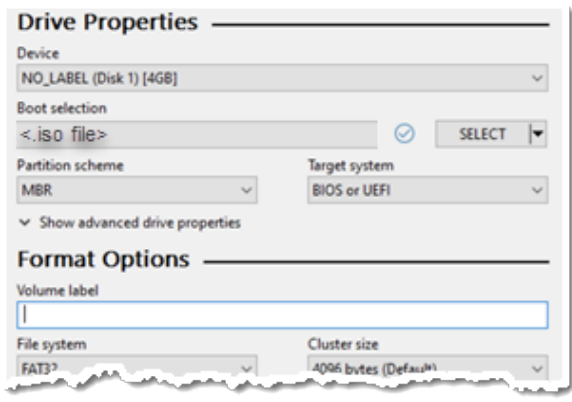
Before you begin

Ensure that the USB flash drive meets the following minimum requirements:

- USB Standard 2 or 3
- USB Connector Type-A

Procedure

The USB flash drive preparation steps vary somewhat between Ivanti EPMM 11.3.1.0 and older releases from Ivanti EPMM 11.4.0.0 - 11.12.0.0 and newer releases. Follow the steps for your release:

TABLE 22. USB FLASH DRIVE PREPARATION STEPS, BY RELEASE

Step	Installation prep for Ivanti EPMM 11.3.1.0 and older releases	Installation prep for Ivanti EPMM 11.4.0.0 and newer releases
1	Insert a USB flash drive into a Windows PC. Use a USB flash drive with a minimum of **2 GB** storage space.	Insert a USB flash drive into a Windows PC. Use a USB flash drive with a minimum of **4 GB** storage space.
2	Download the Ivanti EPMM ISO image to the same PC from the Ivanti EPMM Support site.	Download the Ivanti EPMM ISO image to the same PC from the Ivanti EPMM Support site.
3	Download a third-party tool to the same PC to create a bootable USB flash drive. Ivanti EPMM uses the tool **Rufus** for creating bootable USB drives, which can be downloaded here: https://rufus.akeo.ie/.	Download a third-party tool to the same PC to create a bootable USB flash drive. Ivanti EPMM uses the tool **Rufus** for creating bootable USB drives, which can be downloaded here: https://rufus.akeo.ie/.
4	Run the tool and provide the following information when asked in the tool wizard: • Location of the ISO. • Location of the USB flash drive. • Volume label name for the USB flash drive. You must use **MOBILEIRON** as the volume label name.	Run the tool and provide the following information when asked in the tool wizard: • Location of the ISO. • Location of the USB flash drive. • Leave the Volume label **empty**, as shown below: **Drive Properties** Device NO_LABEL (Disk 1) [4GB] Boot selection <.iso file> SELECT Partition scheme Target system MBR BIOS or UEFI ˅ Show advanced drive properties **Format Options** Volume label File system Cluster size FAT32 4096 bytes (Default)
5	Select: • **Partition Scheme: MBR** and	Select: • **Partition Scheme: MBR** and

TABLE 22. USB FLASH DRIVE PREPARATION STEPS, BY RELEASE (CONT.)

Step	Installation prep for Ivanti EPMM 11.3.1.0 and older releases	Installation prep for Ivanti EPMM 11.4.0.0 and newer releases
	• **Target System: BIOS** or **UEFI**	• **Target System: BIOS** or **UEFI** Master Boot Record (MBR) Basic Input/Output System (BIOS) Unified Extensible Firmware Interface (UEFI)
6	For File System, select **FAT32**.	For File System, select **FAT32**.
7	Complete the wizard to create a bootable USB flash drive.	1. Click **Start**. 2. **ISO Hybrid image detected** popup menu displays. 3. Select **Write in DD image mode**, as shown below: Please select the mode that you want to use to write this image: ○ Write in ISO Image mode (Recommended) ◉ Write in DD Image mode OK 4. Click **OK**. Allow the Wizard to complete the bootable USB drive.
8	Continue to "Installing the Ivanti EPMM ISO image on M2250 and M2600 appliances" on page 47 for installation instructions. When requested during the installation, select **hw-m2250-m2600-usb-install**.	Once the bootable USB drive is complete, continue to "Mounting and installing the Ivanti EPMM ISO image on an M2700 appliance" on the next page for installation instructions. When requested during the installation, select **Install Ivanti EPMM 11.4.0.0-xx from USB**.

ℹ Installation of Enterprise Connector on M2250, M2600, and M2700 appliances via USB is not supported.

Mounting and installing the Ivanti EPMM ISO image on an M2700 appliance

The procedures for mounting the Ivanti EPMM ISO image have changed with the introduction of the Ivanti EPMM M2700 appliance and the Ivanti EPMM 11.4.0.0 release. The mounting process occurs from the Intel® Integrated baseboard management controller web console (BMC console) using the Intelligent Platform Management Interface (IPMI) 2.0 SOL protocol.

See "M2700 Series appliance" on page 82 for specifications for this appliance.

> **ⓘ** A Java Runtime Environment (JRE) is required for the following steps, unless HTML5 is supported by your browser, and a JRE is not installed.

Procedure

1. Navigate to the BMC console.

2. Click the **Remote Control** tab and select **KVM Console Redirection**.

3. From the KVM/Console Redirection page, click **Launch Console**.

   > **ⓘ** Systems that do not have a valid Java Runtime Environment (JRE) installed use HTML5. The following steps require a JRE.

4. A Java Network Launch Protocol (JNLP) file is downloaded to your local device. Save the file at the prompt.

5. Open **launch.jnpl** (the file that was downloaded). When a security warning opens, click **Continue**.

6. Another security warning opens, warning of possible security risks by allowing these types of applications to run on your machine.
   Click **I accept the risk and want to run this application**, and click **Run**.

7. In the pop-up window, enter your BMC log in credentials, and click **Login**.

8. Another warning opens: "**JCE Unlimited Strength Jurisdiction Policy Files required by AES-256 are not installed on the client side. Switch to AES-128 instead**."
   Click **OK**.

9. A console screen opens. In the upper-left, click **Virtual Media** > **Virtual Storage**.

10. A Virtual Storage pop-up window opens. Provide the following settings for the virtual storage devices:

    a. **Logical Drive Type**: Select **ISO File**.

       The Image File Name and Full Path field is enabled.

    b. **Image File Name and Full Path** : Click **Open Image**.

       You must have previously downloaded a copy of the ISO image to your local device to populate the image this way. The Ivanti EPMM image begins mounting on the Ivanti EPMM M2700 appliance. When complete, the connection status displays in the **Connection Status History** field.

11. After mounting, reboot the appliance using the console screen command **Power Control** > **Power Reset**.

12. After rebooting, a menu window opens, asking you to select the boot device. If you mounted the ISO via Virtual Media, it's going to appear as a Virtual CDROM. If a USB stick is plugged into the server, then it will show a USB device.

    Select the option **UEFI USB 2.0 USB Flash Drive 0.00** and **Enter**.

13. From the console screen, use the arrow keys to select the correct option for your installation:

    • **IPMI**: **Install Ivanti EPMM 11.4.0.0-*xx***

    • **USB**: **Install Ivanti EPMM 11.4.0.0-*xx* from USB**

14. Click **Enter**. Ivanti EPMM begins installing on your M2700 appliance. A successful installation displays the Ivanti EPMM CLI banner on the console. The installation script continues, displaying status on the console. This may take several minutes.

Installing the Ivanti EPMM ISO image on M2250 and M2600 appliances

The following steps describe the installation of the Ivanti EPMM software.

Before you begin

1. Connect a monitor and keyboard to the Ivanti EPMM appliance.

2. Power on the appliance to boot the system.

3. If you are using a USB flash drive to install Ivanti EPMM ISO to an M2250 or M2600 appliance, ensure that you have prepared the USB flash drive as described in "Preparing a USB flash drive for installation" on page 43.

Procedure

1. Insert the DVD or USB flash drive (containing the Ivanti EPMM ISO image) into the appliance.

2. Wait for the appliance to reboot for the installation program to begin after a few minutes.

3. Enter the command for the installation you want to complete:
   - **vm-install**: for a virtual Ivanti EPMM.
   - **hw-install**: for any standard physical appliance.
   - **hw-m2250-m2600-install**: for physical appliance installation on the M2250, or M2600 appliances.
   - **hw-m2250-m2600-usb-install**: for installing Ivanti EPMM from a USB flash drive onto the M2250 or M2600 appliances.

4. Press **ENTER** to start the installation process.

5. In the Welcome wizard type **yes** to display the end user license agreement.

6. Scroll through and read the agreement.

7. Type **yes** to accept the End User License Agreement.

8. Enter the **company name**.

   The company name you enter will serve as the default enterprise name used in SMS and email communication.

9. Enter the **name** of the person in your organization who will serve as the contact point for Ivanti EPMM communications.

10. Enter the **email address** for the contact person.

11. Enter the new **password**.

    The password must be between 6 and 20 characters.

12. **Re-enter** the password.

13. Enter the user name you want to assign for the **first administrative user**.

    > ℹ️   Do not use `root` or or `ha_admin`.

14. Enter the **password** you want to assign for the administrator.

    This password must contain at least 8 characters and include numerals and capital letters.

15. **Re-enter** the administrator password.

16. Enter the **letter** for the physical interface you want to use to connect to the management network.
    a. for GigabitEthernet1
    b. for GigabitEthernet2

17. Enter the **IP address** that you created for Ivanti EPMM.

    It will be associated with the physical interface you selected in the previous step.

18. Enter the **netmask** for use with the IP address you just entered, for example, 255.255.255.0.

19. Enter the **default network gateway** for Ivanti EPMM.

20. Enter the **external hostname** (fully-qualified domain name) for the appliance.

    > ℹ️ Do not use an internal hostname. Managed devices must be able to access Ivanti EPMM from the Internet.

21. Enter the **IP address** of the primary name server to be used by Ivanti EPMM.

22. Enter optional secondary and tertiary name servers as preferred.

    Leave the fields blank and press **Enter** to skip specifying additional name servers.

23. Enter **yes** to enable remote access via SSH.

24. Enter **yes** to configure an optional reliable time source at the Configure NTP prompt.

    We recommend that you configure at least one time source to ensure proper synchronization of time-based tasks.
    - If you entered yes for configuring a time source, enter the IP address of the primary time source to use.
    - If you specified a time source, you can enter secondary and tertiary time sources.
    - If you do not specify at least one time source, then you have the option to configure the system clock.

25. If prompted, enter **yes** to configure the system clock's time and date.

    - Use **HH:MM:SS** as the format for the time you enter.
    - Use **DD MM YYYY** as the format for the date you enter.

26. **Review** the displayed command script.

27. Enter **yes** to save the changes.

    When the configuration is complete, the installation program displays the **Configuration complete** message.

28. Enter **reload** to reboot the system and enable the portal service.

29. Enter **yes** when prompted to save the system configurations.

30. Enter **yes** to proceed with reload.

    A successful installation displays the Ivanti EPMM CLI banner on the console. The installation script continues, displaying status on the console. This may take several minutes.

Signing in to the Ivanti EPMM System Manager

You can sign in to the Ivanti EPMM System Manager directly from a web browser or from the Ivanti EPMM 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.

Procedure: From a browser

1. Open a supported browser.

2. Enter https://<fully-qualified_domain_name>:8443/mics.

3. Enter the administrator user name and password you specified in the configuration wizard.

Procedure: From the Ivanti EPMM Admin Portal

1. Log into the Ivanti EPMM Admin Portal.

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

3. Select **System Manager** from the menu.

4. Log into System Manager to open the System Manager workspace.

Next steps

- "Configuring email integration" below
- "Changing port settings" on the next page
- "Setting up local administrator users" on page 53
- "Restricting access to Ivanti EPMM components" on page 53
- "Rolling out Ivanti EPMM" on page 53
- "Updating Ivanti EPMM software" on page 53

Configuring email integration

Use the Email Settings screen in the System Manager portion of the portal to set up the 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.

Procedure

To configure email integration:

1. Log into System Manager.

2. Go to **Settings > Email Settings**.

3. Edit the fields, as necessary.

4. Refer to the "Email configuration window" on the next page table for details.

5. Click the **Test** button to open the **Test Email** window.

6. Enter an email address and body for the test email.

7. Click **Send**.

8. Confirm that the email arrived.

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

Email configuration window

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

TABLE 23. EMAIL CONFIGURATION FIELDS

Fields	Description
From Email	Specify the email address to use in the From field for all administrative email notifications. Make sure that the email address has the right privileges to send emails to internal and external email domains.
SMTP Server	Specify the IP address or fully-qualified host name for the SMTP server the Ivanti EPMM 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 **SMTPS** button. Otherwise, leave **SMTP** selected. If you want to allow an existing connection to upgrade to an encrypted connection, select **SMTP with STARTTLS.**
Authentication Required	Specify whether this SMTP server requires authentication. In most cases, this field will be set to **Yes**.
User Name	If you select **Yes** for **Authentication Required**, then this field displays. Enter the user name required for SMTP authentication.
Password	If you select **Yes** for **Authentication Required**, then this field displays. Enter the password required for SMTP authentication.
Confirm Password	If you select **Yes** for **Authentication Required**, then this field displays. Confirm the password required for SMTP authentication.

Changing port settings

The default provisioning port is HTTP/8080. If you have signed certificates, you can select HTTPS/443, instead.

Procedure

1. Log into the System Manager.

2. Go to **Settings > Port Settings**.

3. Select **https**.

4. Click **Apply > OK**.

Setting up local administrator users

Local administrators have access to the configuration of the server. The initial setup created the first local administrator user.

- To create new users go to **Security > Local users > Add**.

- To create user accounts for the Admin Portal, including accounts to register devices, see the "Managing Users" chapter in the *Ivanti EPMM Delegated Administration Guide*.

Restricting access to Ivanti EPMM components

We recommend specifying either a singular IP or a network ID and subnet for Smartphone Manager access. You can also restrict access for other components of Ivanti EPMM. To configure these restrictions, select Security > Portal ACL in System Manager. See the Ivanti EPMM System Manager Guide for details.

Rolling out Ivanti EPMM

See the Ivanti EPMM Device Management Guide for guidelines for planning the next steps, including setting up policies and registering devices.

Updating Ivanti EPMM software

Get Ivanti EPMM software updates, as necessary. See the **System Manager Guide** for the specific release for instructions about how to upgrade to the release.

Installing Enterprise Connector

This chapter includes the following sections:

About the Enterprise Connector

The Enterprise Connector is a component that connects Ivanti EPMM to corporate directories, such as Microsoft Active Directory or LDAP, by means of secure HTTPS connections. Multiple connectors can be used for scaling and redundancy purposes. Requests go to all configured Connectors, but only one responds to the request. Should one fail, all the requests are handled by another working Connector.

> The Ivanti EPMM Connector does not support certificate-based authentication. This means that once you enable Connector service, the **Upload X509 Certificate** option in LDAP preferences is not available.

> The Enterprise Connector is not domain-specific and therefore every connector must be able to reach every LDAP server.

Installation and configuration tasks

Complete the following tasks to install and configure the Enterprise Connector:

1. Complete preparations listed in Chapter 1, .

2. Configure the Enterprise Connector on Ivanti EPMM ().

3. Install the Enterprise Connector ISO package ().

4. Install the Enterprise Connector with the Configuration Wizard ().

5. Configure the Enterprise Connector ().

6. Verify the Ivanti EPMM connection ().

Virtual Enterprise Connector requirements

If you are installing a virtual Enterprise Connector, ensure that the minimum requirements described in this section are met.

Storage devices

The table below lists the requirements for storage devices.

TABLE 24. STORAGE DEVICE REQUIREMENTS

Operation	Min IOPS	Bandwidth	90% Operations < xxx mS
Random Read	400	3 MBps	10 mS
Random Write	900*	15 MBps	4 mS

* RAID controller may have to be specifically configured in order to achieve high Random Write IOPS - (e.g. Disk Cache: Enabled, Default Write: Write Back with BBU)

ℹ️ Ivanti recommends configuring only one hard drive per virtual machine.

System performance is directly related to storage device performance. We recommend using only high-performance tier 1 storage products.

Enterprise Connector components

The following table lists the requirements for the following Enterprise Connector components.

TABLE 25. ENTERPRISE CONNECTOR COMPONENT REQUIREMENTS

Components	Requirements
Hard drive	We recommend configuring only one hard drive on the virtual machine. System performance is directly related to hard disk drive performance. We recommend using only high-performance tier I storage products.
Backup VMware	Ivanti recommends taking periodic .vmdk backups of your Virtual Appliance as part of your system maintenance. Use VMware VCB or another VMware-supported backup system. A backup of the full virtual disk is recommended; VMware snapshots are not sufficient.

VMware	Confirm the following requirements before beginning setup of the Virtual Enterprise Connector:
	
	• VMware ESXi versions 6.5, 6.7, 7.0 with data stores created
	• 64-bit VM
	• 2 GB Memory
	• 40 GB Disk
	• Two CPU cores with min clock rate of 2 GHz
	• Boot from BIOS firmware
	• Network adapter
	
	    ◦ E1000
	    ◦ VMXNET 3
	
	• VM OS Type: CentOS 7.4 (64-bit)
	
	    ℹ️ This setting is intended to ensure successful installation; it does not imply that Ivanti distributes Red Hat.
	
	• CPU Settings:
	
	    ◦ Shares: Normal
	    ◦ Reservation: 900 MHz
	    ◦ Limit: Unlimited (maximum assigned)

TABLE 25. ENTERPRISE CONNECTOR COMPONENT REQUIREMENTS (CONT.)

Components	Requirements

	• Memory Settings:
	
	  ○ Shares: Normal
	
	  ○ Reservation: 1.5 GB
	
	  ○ Limit: Unlimited (maximum assigned)

Hyper-V	• Download link or package (ISO) from Ivanti EPMM Support https://support.ivanti.com/support/CDL.html • Microsoft Hyper-V Server 2008, Microsoft Hyper-V Server 2008 R2 Microsoft Hyper-V Server 2012, Microsoft Hyper-V Server 2012 R2 Microsoft Hyper-V Server 2016 • 64-bit Generation 1 VM • 2 GB Memory • 20 GB Disk • Two CPU cores with min clock rate of 2 GHz • Boot from BIOS firmware • Minimum 4 GB RAM • Network adapter * Microsoft Hyper-V Server 2008 requires legacy network adapter

KVM	Connector can run on a Kernel Virtual Machine (KVM) as follows:
	
	• Download link or package (ISO) from Ivanti EPMM Support at
	https://support.ivanti.com/support/CDL.html
	
	• Minimum configuration of host machine:
	
	  ○ Quad Ivanti EPMM CPU with min clock rate of 2 GHz
	  ○ 16 GB RAM
	  ○ 8 GB guest memory:
	
	  ⓘ Performance data for different CPU, RAM, and memory configurations is not available.
	
	• **Supported KVM version**: QEMU emulator version 2.0.0 (Debian 2.0.0+dfsg-2ubuntu1.22)
	Ivanti EPMM supports only this KVM version, but later versions are compatible.

TABLE 25. ENTERPRISE CONNECTOR COMPONENT REQUIREMENTS (CONT.)

Components	Requirements
	• **Supported Virtual Machine Manager version**: 0.9.5 Ivanti EPMM supports only this Virtual Machine Manager version, but later versions are compatible.* • **Supported Linux distribution**: Ubuntu Server version 14.04 Ivanti EPMM supports only this Linux distribution, but other Linux distributions are compatible. • In the **Virtual Machine Manager**, when creating a new virtual machine, select **Generic** for the OS type and the Version. • Boot from BIOS firmware ⓘ For more information about setting up KVM, see https://help.ubuntu.com/community/KVM. * For definitions of supported and compatible versions, refer to the latest Ivanti EPMM release notes.

Gather required Enterprise Connector information

Enterprise Connector is an optional alternative for integrating with your network. Use the following table to gather and record Enterprise Connector information before installation.

TABLE 26. ENTERPRISE CONNECTOR INFORMATION

Item	Description	Values
Licensing agreement information	The company name, contact person name, and contact person email address for the end-user licensing agreement.	
IP Address	IP address defined for the Connector and the corresponding netmask.	
Hostname	Fully-qualified domain name for the Connector.	
"enable secret" password	The Ivanti EPMM password to be defined for enabling access to Privileged and Configuration modes.	

TABLE 26. ENTERPRISE CONNECTOR INFORMATION (CONT.)

Item	Description	Values
Administrator User Name	The user name to define for the Ivanti EPMM administrator.	
Administrator Password	The Ivanti EPMM Administrator password must contain the following elements: • At least 8 characters. • At least 1 alphabetic character. • At least 1 numeric character. • Cannot have 4 or more repeating characters. • Cannot be the same as the user ID. • May contain Unicode characters, except for CLI access. Users cannot change a password more than once during a 24 hour period.	
Physical Interface	The physical interface to use. Enter a or b.	
Default Gateway	The IP address of the router used to forward traffic to destinations outside of the local network or subnet.	
Name Server 1, 2, 3	The IP address of a network name server (a DNS server, for example). You must specify at least one name server.	
Remote Shell via SSH?	Specifies whether you want to configure remote shell access via SSH.	
NTP Server 1, 2, 3	Specifies the IP address of an optional reliable time source. We recommend specifying an NTP server. If you do not, you will have the opportunity to set the system clock and date.	

Configuring Ivanti EPMM for an Enterprise Connector

There are several tasks that need to be completed on Ivanti EPMM prior to Connector installation. This section contains the following tasks:

- Assigning the Connector role
- Adding Enterprise Connector entries

- Setting Enterprise Connector preferences

Assigning the Connector role

Each Connector authenticates to Ivanti EPMM with an Authorized Admin Portal local user account. We recommend creating a user and assigning only the **Connector** role to authenticate the Connector to your Ivanti EPMM.

> ℹ️ If you are using multiple Connectors and/or auditing tools that require user names, assign one user account to each Connector rather than having one user account accessing all Connectors.

Procedure

1. Log on to the Admin Portal: https://<fully-qualified_domain_name>/admin

2. Select the **Devices & Users > Users**. Click **Add Local User**.

3. Enter the requested information to create the user account for Connector access.

4. Click **Save**.

5. Go to **Admin > Admins**.

6. Select the local user you created for Connector access.

7. From **Actions**, select **Assign to Space**.

   Ivanti EPMM displays the Assign to Space dialog.

8. From **Select Space**, select the device space for this user.

   See *Ivanti EPMM Delegated Administration Guide* for information about device spaces and roles.

9. In the **Admin Roles** section of Assign to Space, find **Other Roles**.

10. In **Other Roles**, check **Connector**.

11. Click **Save**.

12. Continue to Adding Enterprise Connector entries

Adding Enterprise Connector entries

You can add a maximum of ten Connector entries on Ivanti EPMM.

Procedure

1. Log on to the Admin Portal: https://<fully-qualified_domain_name>/admin

2. Select **Services > Connector**.

3. Click **Add New**.

4. **Name** - Enter a name for the Connector. You will need this name when you configure the Connector.

5. **Enabled** - Set to **Yes** to allow this Connector to provide services to Ivanti EPMM, including allowing Ivanti EPMM to use Connector for Lightweight Directory Access Protocol (LDAP) queries.

6. Click **Save**. The Connector status will remain **Stale** until the Connector is configured as described in "Configuring Enterprise Connectors" on page 67.

7. Select the Connector to display the detailed information on the right pane.

8. Record the URL. You will need it when you are Configuring Enterprise Connectors.

   ℹ️ "Not Available" displays on the Connector Detail Page, because the Connector has not yet been configured.

9. Continue to Setting Enterprise Connector preferences.

Setting Enterprise Connector preferences

After you have added at least one Enterprise Connector, you can set Connector default preferences.

ℹ️ Preference choices affect all Connectors; they cannot be individually configured.

FIGURE 1. ENTERPRISE CONNECTOR PREFERENCES MENU

Before you begin

Complete Adding Enterprise Connector entries before setting preferences.

Procedure

1. Log on to the Admin portal.

2. Select **Services > Connector**.

3. Click the **Preferences** link to open the Preferences menu.

   a. **Connector Services**: Click **Enable**. When enabled, services communicate through Connectors instead of directly communicating with their respective servers.

   > ℹ️ Connector Services *must* be enabled for Ivanti EPMM to use Enterprise Connector for Lightweight Directory Access Protocol (LDAP) queries.

   b. **Status Reporting Interval**: Set an interval time between 1-59 minutes, or leave the default 15 minutes.

   c. **LDAP Timeout**: Set a timeout value between 1 and 3600 seconds, or leave the default 25 minutes.

   d. **LDAP Request Retries**: Leave the default number of retries (1) or set this value to **0** to disable LDAP request retries. Do not set this value to other than 1 or 0 without explicit direction from Ivanti Support or a knowledge-based article.

e. **LDAP Test Timeout**: Leave this value at 25 seconds. Do not change this value without explicit direction from Ivanti Support or a knowledge-based article.

f. **LDAP Request Batch Size**: Leave this value at 100 per LDAP batch request. Do not change this value without explicit direction from Ivanti Support or a knowledge-based article.

4. When done, click **Save**. A pop-up message confirms the save.

Installing the Enterprise Connector ISO package

After the VM environment is set up, you can install the Connector ISO package.

Procedure

1. Log into the VM Client.

2. In the directory tree on the left, right-click the device for which you want to install the package.

3. Select **Edit Settings** from the drop-down menu.

4. Select **CD/DVD Drive 1**.

5. Click the **Datastore ISO File** option.

6. Click **Browse** and navigate to the directory where the ISO package is kept.

7. Select the ISO package.

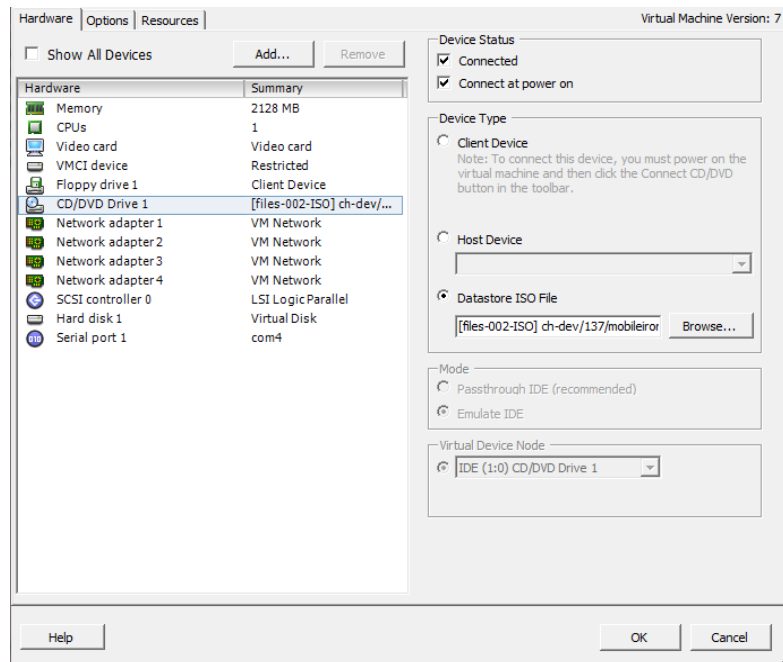8. Click **Open** to return to the **VM Properties** screen.

9. Click **OK** to return to the previous screen.

10. Right-click the device for which you will install the package.

11. Select **Power**, then **Reset**.
    You are prompted to confirm that you want to proceed

12. Click **Yes** to reset the virtual machine.
    The installer checks and formats the file system.

13. Observe the status messages at the bottom of the screen.
    The VM automatically installs and reboots after a few minutes, after which it displays the configuration screen.

14. Click the **Console** tab to specify the type of services you want to install.

15. Type **vm-install**.
    The installer performs several minutes of file system formatting and image installation. When this step is finished, the installer starts the configuration wizard.

16. Continue the installation with the configuration wizard.
    See "Installing with the Configuration Wizard" below for details.

Installing with the Configuration Wizard

After you install the Enterprise Connector ISO package, the Welcome screen is displayed.

Procedure

1. Enter **yes** to continue and to open the end user license agreement.

2. Scroll through and read this agreement.

3. Enter **yes** when asked to accept the agreement or **no** to close the Wizard and terminate the installation process.

4. Enter the following information:
   - company name used in both the SMS and email communication
   - contact person's name
   - contact person's email

5. When asked to **Enter enable a secret**, enter a password between 6 and 20 alphanumeric characters. The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, is encrypted in the configuration.

6. Re-enter the password at the confirmation prompt.

7. Enter the **Administrator User Name** at the prompt.

8. Enter the **Administrator Password** at the prompt.

9. Enter the network interface you will use to connect to the management network.

10. Type **a** or **b** for the physical interface you want to use.

11. Enter the **IP Address** associated with the physical interface you selected.

12. Enter the **Netmask** associated with the IP address you just entered.

13. Enter the IP of the **Default Gateway** for the appliance.

14. Enter the hostname of the appliance.

    Although the Wizard requests an External Hostname (FQDN) for this step, Connector does not require an externally accessible URL, and therefore, you can enter an internal or external hostname.

15. Enter the IP address of the primary name server (**Name Server 1**) used by the appliance.

16. Enter the IP address(es) of the secondary and tertiary name servers, as preferred, or press **Enter** to skip adding more name servers.

17. Type **yes** to enable **remote shell access via SSH** or **NO** to disable this option.

18. Type **yes** to enable **NTP** or **NO** to disable this option.

19. Enter the IP address of the primary time.

20. Enter the IP address(es) of the secondary and tertiary time source(s) or press <Enter> to skip adding more time sources.

21. Type **yes** to save your changes.

22. Type **reload** to reboot the system and enable the portal service.

23. Type **yes** when asked if you want to proceed with reload.

    The installation script continues, displaying status on the console. The installation process may take several minutes. When it is complete, a confirmation message displays.

Configuring Enterprise Connectors

After the Enterprise Connector is installed and configured on Ivanti EPMM, you can configure the settings on the Connector. 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.

Procedure

1. Gather the following information from "Adding Enterprise Connector entries " on page 61:
    - **Name**: The name you gave the Enterprise Connector
    - **URL**: The URL that you copied from the Enterprise Connector detailed information earlier.
    - **User ID/password**: The one to which the Connector role was assigned in "Assigning the Connector role" on page 60.

2. Log in to the Connector (`https://<fully-qualified_domain_name:8443>/mics`).

3. Select **Connector** from the left panel to open the Connector Settings page.

4. Enter the Connector name in the **Name** field.

    > **i** The Connector name must match the name created on Ivanti EPMM. It is case sensitive.

5. Enter the Connector URL in the corresponding field.

6. Select **Yes** for private deployment that accepts the self-signed certificates. The default is **No**. Contact Customer Support for more information.

7. Enter the user ID and password in the respective fields.

    > **i** This is the Connector user and role created on Ivanti EPMM.

8. Re-type to confirm the password.

9. Click the check box for **Outbound Proxy Required**. Use the following guidelines to specify the settings:

TABLE 27. OUTBOUND PROXY SETTINGS

Item	Description
Proxy Host Name / IP	Enter the Proxy server host name or IP address.
Proxy Port	Enter the port on which the Proxy server is listening. The default is set as 8080.
Proxy Authentication Required	Click the check box if authentication is required for the proxy server. ⓘ Only HTTP basic authentication is supported.
Proxy User ID	Enter the User ID for the proxy server.
Proxy User Password	Enter the password for the proxy server.
Proxy User Confirm Password	Re-enter the password.

10. Click **Apply**. A dialog appears prompting you to confirm that you want to proceed.

   ⓘ   **Apply** saves the configuration in the current session only. It is not persistent after the machine reboots.

11. Click **OK** to return to the Connector Configuration page.

12. Click **Save** in the upper-right corner to make the configuration persistent after the machine reboots.

   ⓘ   The configuration must be saved before it can be tested.

13. Click **Test** to validate the configuration. A dialog appears displaying the status.

Verifying the Ivanti EPMM connection

After the Connector is configured, confirm that it is connected to Ivanti EPMM:

Procedure

1. Log on to the Admin Portal: `https://<fully-qualified_domain_name>`

2. Go to **Services > Connector**.

   The Connector page opens displaying the Connection status.

   > ℹ️ Both More Actions and View Global Statistics menus are used in conjunction with Ivanti EPMM personnel for diagnostics purposes.

3. Click the Connector of interest to display the detailed information on the right pane.

   > ℹ️ Troubleshooting and View Statistics are used in conjunction with Ivanti EPMM personnel for diagnostics purposes.

Understanding global statistics

The following table describes the values tracked in the Global Statistics pane:

TABLE 28. GLOBAL STATISTICS

Statistic	Description
work	Statistics related to work orders posted by Ivanti EPMM, for example, an LDAP query from Ivanti EPMM is a work order from Ivanti EPMM to Connector.
posted	Number of work orders posted to Connector.
async	Number of asynchronous work orders posted from Ivanti EPMM.
solicitTimedout	The solicit is the empty request posted from Connector. Ivanti EPMM sends a work order in response to the solicit if the work order is queued. Timeout means the solicit pended until the timeout limit and Ivanti EPMM did not have any work order to post in response, therefore, it abandoned the solicit.
responseTimedout	Connector could not respond to the work order within the time Ivanti EPMM was expecting resent work orders reposted.

TABLE 28. GLOBAL STATISTICS (CONT.)

Statistic	Description
noConnectors	Ivanti EPMM did not process work orders because there are no corresponding solicits from Connector, or connector is off-line.
validationFailed	Internal processing error.
dispatchLatency	The latency required to dispatch the work orders, with min, max, and ave calculated using the specified number of work orders.
responseLatency	The time required to get the response from Connector after posting the work order to Connector.
realtimeCounters	
pendingSolicits	Current number of waiting solicits in the queue from Connector waiting for work orders.
pendingWorkOrders	Current number of pending work orders in the queue waiting for Connector solicits.

Configuring LDAP servers

You can configure multiple LDAP servers, but each server must contain a unique LDAP configuration.

Procedure

1. Log on to the Admin Portal: https://<fully-qualified_domain_name>/admin.

2. Select **Services > LDAP**.

3. Click **Add New** to open the New LDAP Setting page.

4. Enter information in the following fields to set up a connection to the LDAP directory:

   - Directory URL: Enter the URL to the LDAP server. Make sure to start with "ldap://" or "ldaps." You do not need to specify the ports when you use these default ports: 389 (LDAP) or 636 (LDAPS).

   - Directory Failover URL: Enter a secondary URL, if available.

   - Directory UserID: Enter the primary user ID, for example, userid@local.domain.

     > ℹ️ Make sure to include the domain, e.g., @local.domain, with the user ID.

- Directory Password: Enter the password for the user ID set above.

- Search Results Timeout: Leave it at the default of 30 seconds; unless you get connection errors.

- Connect Timeout: Leave it at the default of 30 seconds; after 30 seconds, it looks for other LDAP servers.

- Chase Referrals:

  a. Select **Enable** if you are using a multi-forested domain. This indicates you want to use alternate domain controllers when the targeted domain controller does not have a copy of the requested object.

  b. Select **Disable** if you do not use alternate domain controllers.

    > ℹ️ Enabling the Chase Referrals option delays LDAP authentication.

- Admin State: Select **Enable** to put the server to service.

    > ℹ️ Make sure you enable the Admin State or the LDAP server will be invisible.

- Directory Type:

  a. Select **Active Directory** for the Microsoft Windows server platform.

  b. Select **Domino** for the IBM Lotus Domino server platform. The default DN and other LDAP search filters are automatically changed to the Domino server.

  c. Select **Other** for other platforms.

- Domain: Enter the domain name for the Active Directory. This information will automatically traverse all levels of the tree and use them to populate Base DN, parent entry.

5. Enter information in the following fields to set up a connection to the Directory Configuration Domain Components:

- DC Base DN: Enter a DN that is high enough in the directory's structure to show domain components.

- DC Search Filter: Enter your search criteria.

6. Enter information in the following fields to set up a connection to the Directory Configuration Organizational Unit:

   - OU Base DN: Enter a DN that contains the appropriate organizational units.

   - OU Search Filter: Enter your search criteria.

7. Enter information in the following fields to set up a connection to the Directory Configuration Users:

   - User Base DN: Enter user base distinguished name, if available.

   - Search Filter: Enter your search criteria.

   - Search Scope: Select **All Levels** from the drop down.

   - First Name: Enter the first name.

   - Last Name: Enter the last name.

   - User ID: Enter the user id.

   - Email: Enter the email address.

   - Enter the information in the following fields (Display Name, Distinguished Name, User Principal Name, and Locale)

   - User Security Identifier: Enter objectSid to read the objectSID value from the LDAP user. Only when **Active Directory** is selected.

8. Click **View LDAP Browser** to view the LDAP server directory tree structure.

9. Click **Test**.

10. Enter a user or group identifier in the appropriate field.

11. Click **Submit** to display a result page if the user was configured on the LDAP server.

```
Found the user with user id 'training9'
First Name : Doris
Last Name : Lok
User ID : training9
Email : dlok@mobileiron.com
```

12. Return to the LDAP page and click **Save**. A dialog appears concerning traffic disruption and prompts you to confirm that you want to proceed.

13. Click **Yes**. A dialog appears listing the status.

14. Click **OK**. The server you created appears on the LDAP page.

> Ivanti EPMM is unable to resolve multiple LDAP entries with the same identifier (SAMAccountName). We recommend you use globally unique identifiers for each entry across LDAP forests.

After implementing the channel-binding LDAP signing requirements, you now have two options:

- LDAP -- Select this option for standard LDAP security. This is the Connector default. Go to **Services > Trusted Certificates > Select/Show Untrusted certificate**. From the **Actions** menu, mark the certificate as trusted.

- LDAPS -- Select this option for Strict SSL security. From the LDAP preference section, upload the CA certificate into the connector.

Manually upgrading Enterprise Connector

In most cases, Enterprise Connector is upgraded automatically after a Ivanti EPMM upgrade. Ivanti EPMM upgrades include any new service package necessary for the Enterprise Connector. If Connector needs to be updated, then Ivanti EPMM prompts Connector to access the new package and complete an in-place upgrade. In most cases, this process completes successfully, and Connector restarts.

If there is a problem with the in-place upgrade, then Connector makes two additional attempts to complete the upgrade. Connector reboots before attempting to upgrade again. If the upgrade is still not successful, then Connector reverts to the previous version and begins running in compatibility mode. In this case, you must complete the steps detailed in this section.

Complete the manual upgrade procedure under the following circumstances:

- The automatic upgrade is unsuccessful.
- The current Connector installation requires updates to the host platform.

Procedure

1. In System Manager, select **Maintenance > Software Updates**.

   The default URL should be sufficient. Do not change it unless instructed to do so.

2. Enter the credentials assigned by Ivanti EPMM Support.

3. Click **Apply**.

4. Click **OK** to dismiss the success popup.

5. Click **Check Updates**.

   The available updates are listed.

6. Select the update.

7. Click **Download** if you want to download the update now and complete the installation at a later time.

8. Refresh the screen and click **Check Updates**.

   After the download is complete, the status for the update changes to Downloaded.

9. Click **Stage for Install** when you are ready to install.

   - If you had 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.

10. 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.

11. Select **Maintenance > Reboot** to reboot Enterprise Connector.

    To successfully install the update, you must reboot after the status is **Reboot to install**.

Local user authentication to Enterprise Connector

- "Enterprise Connector user authentication overview" below
- "Certificates required for certificate authentication to Enterprise Connector" on the next page
- "Certificate attribute mapping used in certificate authentication to Enterprise Connector" on the next page
- "Using $EDIPI$ in certificate authentication to Enterprise Connector" on page 78
- "Adding local users to Enterprise Connector" on page 78
- "Add New User window in Enterprise Connector" on page 78
- "Configuring password authentication to Enterprise Connector" on page 79
- "Configuring certificate authentication to Enterprise Connector" on page 80
- "Replacing the certificate for authentication in Enterprise Connector" on page 81

Enterprise Connector user authentication overview

Enterprise Connector administrators are set up as local users in the Enterprise Connector portal in **Security > Local Users**. They can authenticate to the Enterprise Connector portal using one or both of the following methods:

- **A user name and password** - These are the credentials for a local user as set up in the Enterprise Connector portal 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.

- 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 use the Enterprise Connector portal to configure which methods are allowed.

Certificate authentication is also supported in FIPS mode.

Certificates required for certificate authentication to Enterprise Connector

To allow certificate authentication to Enterprise Connector, you upload a PEM-formated file to Connector. The PEM-formatted file contains either:

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

Connector 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 the Enterprise Connector portal, they provide an identity certificate from a smart card. Connector authenticates the user's identity certificate against the certificate that you uploaded to Connector.

> **i** When you create a local user in Enterprise Connector, set the User ID of the local user to the user identity from the identity certificate.

Certificate attribute mapping used in certificate authentication to Enterprise Connector

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

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

TABLE 29. MAPPING INFORMATION USED IN CERTIFICATE AUTHENTICATION

Values	Description	Notes
Designate user identity	Select the user identity field from the identity certificate the authentication. 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, Enterprise Connector uses the User Principal Name in the Subject Alternative Name (SAN) in the identity certificate.
Select a connector substitution variable	The variable against which the authentication compares the user identity. Allowed variables are: • $USERID$ - User ID • $EMAIL$ - Email • $EDIPI$ - EDIPI values entered when configuring the Connector local user.	The $EDIPI$ variable is for the Department of Defense only. See "Using $EDIPI$ in certificate authentication to Enterprise Connector" on the next page. Your choice depends on how you chose to populate the Subject Alternative Name in the identity certificate.

Example

Consider the case in which you specify the NT Principal Name as the field to use from the identity certificate, and you specify $USERID$ or $EMAIL$ as the substitution variable to match. Connector accepts both of the following formats as a match:

- DOMAIN\userid
- userid@domain

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

Related topics

- "Configuring certificate authentication to Enterprise Connector" on page 80
- "Using $EDIPI$ in certificate authentication to Enterprise Connector" on the next page

Using $EDIPI$ in certificate authentication to Enterprise Connector

Using the substitution variable $EDIPI$ is applicable only to Department of Defense customers. You enter it when adding an Enterprise Connector local user. This variable contains the Department of Defense identification number, also known as the Electronic Data Interchange Personal Identifier.

Procedure

If you are a Department of Defense customer setting up authentication to Enterprise Connector using a certificate on a Common Access Card (CAC), then you must:

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

   Make sure the format of the field 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, Connector does not enforce the selection when you configure portal authentication. Connector also does not ensure that you have entered a value into the EDIPI field of the Connector local user.

Adding local users to Enterprise Connector

Only local users created in the Enterprise Connector portal can access the portal. To add a local user to the Enterprise Connector database:

Procedure

1. Log in to the Connector (https://<fully-qualified_domain_name:8443>/mics)

2. Go to **Security > Identity Source > Local Users**.

3. Click the **Add** button to open the **Add New User** window.

4. Modify the fields, as necessary.

   Refer to "Add New User window in Enterprise Connector" below table for details.

5. Click **Apply > OK.**

Add New User window in Enterprise Connector

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

TABLE 30. 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	Enter a password for the user. Valid passwords are determined by the password policy for Enterprise Connector local users at **Security > Identity Source > Password Policy.**
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.
EDIPI	Department of Defense customers only: Enter the user's the Department of Defense identification number, also known as the Electronic Data Interchange Personal Identifier. This field is required if your configuration on **Security > Advanced > Portal Authentication** specifies certificate authentication for access to the System Manager using a common access card (CAC).

Configuring password authentication to Enterprise Connector

You can configure Enterprise Connector to allow administrators to authenticate to Connector with their user name and password.

> ⓘ This authentication method is the default setting.

Procedure

1. Log in to the Connector (https://<fully-qualified_domain_name:8443>/mics)

2. Go to **Security > Advanced > Portal Authentication**.

3. Select **Password Authentication**.

4. Under **Password Authentication**, select **System Manager**.

5. Click **Apply > OK**.

Related topics

"Adding local users to Enterprise Connector" on the previous page

Configuring certificate authentication to Enterprise Connector

You can allow administrators to authenticate to the Enterprise Connector 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 Connector.

Procedure

1. Log in to the Connector (https://<fully-qualified_domain_name:8443>/mics)

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.

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 substitution 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 Enterprise Connector" on page 76
- "Certificate attribute mapping used in certificate authentication to Enterprise Connector" on page 76
- "Using $EDIPI$ in certificate authentication to Enterprise Connector" on page 78

Replacing the certificate for authentication in Enterprise Connector

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

Procedure

1. Log in to the Connector (https://<fully-qualified_domain_name:8443>/mics)

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 Enterprise Connector" on page 76

Appliance specifications

This chapter includes the following sections:

M2700 Series appliance

The Ivanti EPMM M2700 Series large-scale deployment appliance provides a tightly-integrated solution comprised of a standardized appliance with the resources necessary for larger deployments and dedicated QA certification of all Ivanti EPMM functionality. The following table lists the M2700 appliance specifications.

For installation instructions, see "Installing Ivanti EPMM ISO onto an appliance" on page 43.

TABLE 31. M2700 SERIES APPLIANCE SPECIFICATIONS

M2700	Specifications
Form factor	1U Rackmount Chassis, 27.95" D x 1.7" H x 16.93" W
Processors	2 x Intel® Xeon® 6226R, 2.9 GHz, 16-core, 32 cores total
Memory	384GB 2933 MHz DDR4 ECC
USB	2x USB 2.0 Front, 3x USB 3.0 Back
Power	1+1 Redundant 1100W
Management interface	1 x 1GbE RJ-45, IPMI 2.0, RMM4 lite, Virtual media over LAN, KVM over LAN
LAN ports	2 x 10Gbit on-system board Northbridge, 4 x 1Gbit on PCIE 2.1 riser card
Storage devices	4 x 3.2 TB NVMe U.2 Enterprise SSD, RAID10 via Intel VROC

TABLE 31. M2700 SERIES APPLIANCE SPECIFICATIONS (CONT.)

M2700	Specifications
Further information	https://www.intel.com/content/www/us/en/products/sku/192586/intel-server-system-r1208wftysr/specifications.html

M2700 front panel

The following figures, key, and LED table describe the M2700 font panel.
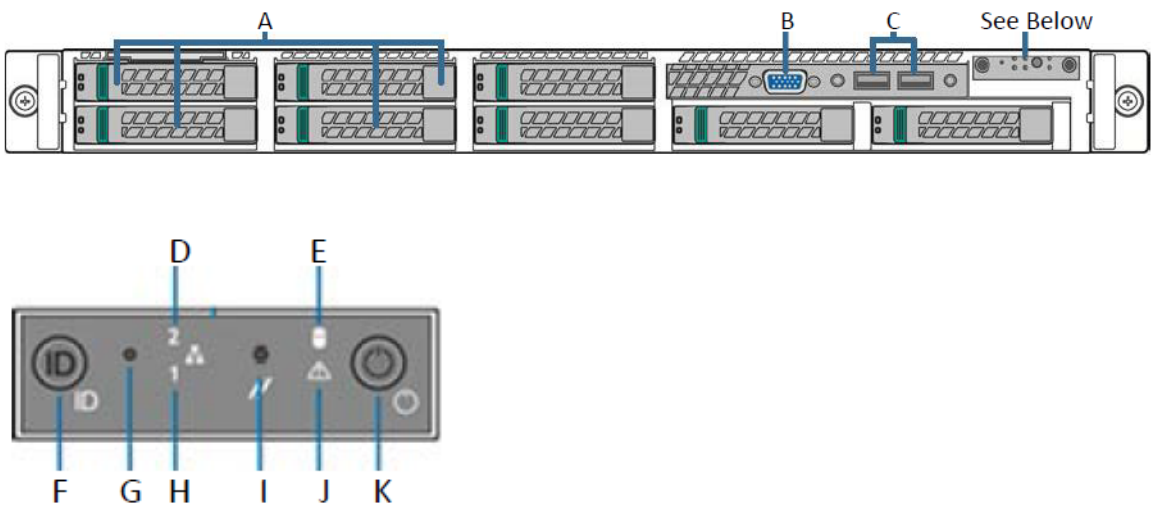
FIGURE 1. M2700 FRONT PANEL

TABLE 32. M2700 FRONT PANEL KEY

A. 3.2TB NVMe SSD	**G**. NMI button
B. Video Port	**H**. NIC-1 activity LED
C. USB Ports	**I**. System cold reset button
D. NIC-2 Activity LED	**J**. System status LED
E. Store drive activity LED	**K**. Power button with LED
F. System ID button with LED	

TABLE 33. INFORMATIONAL LED FIELDS

LED status	Description
Green	OK
Blinking green	Degraded - usually means a redundant part has failed.
Blinking amber	Degraded - System will fail soon
Solid amber	System failure

M2700 back panel

The following figure and key describe the M2700 back panel.
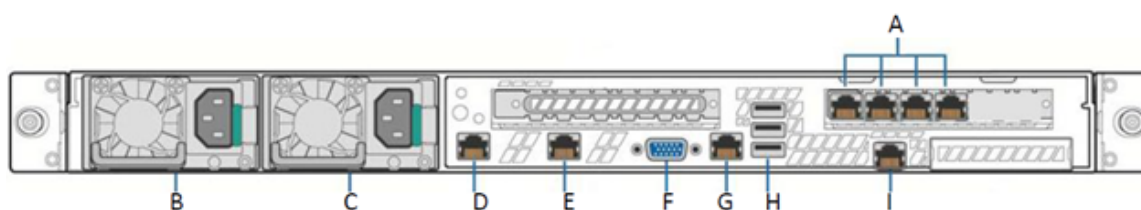
FIGURE 2. M2700 BACK PANEL

FIGURE 3. M2600 BACK PANEL KEY

A. 1G NICs	**F**. Video Port
B. Power Supply 1	**G**. RJ45 Serial Port
C. Power Supply 2	**H**. USB Ports
D. 10G NIC 1	**I**. RMM4 NIC Port
E. 10G NIC 2	

M2600 Series appliance

The M2600 Series large-scale deployment appliance provides the tightly integrated solution of the standard appliance, with the resources necessary for larger deployments. The following table lists the M2600 appliance specifications.
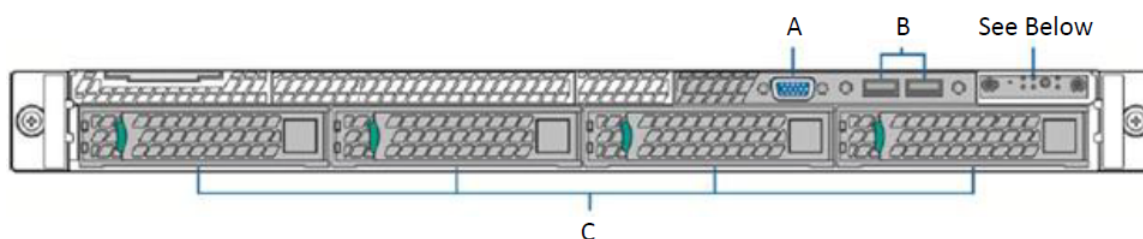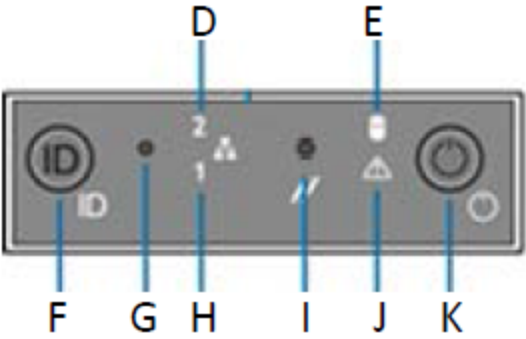
TABLE 34. M2600 SERIES APPLIANCE SPECIFICATIONS

M2600	Specifications
Form factor	1U Rackmount Chassis, 27.95"D x 1.7"H x 17.2"W
Processors	2 x Intel®Xeon® E5-2690 v4, 2600 Mhz, 14 Cores/28 Threads, 28 Cores total
Memory	128 GB, 2400 MHz DDR4 ECC
USB	2x USB 2.0 Front, 3x USB 3.0 Back
VGA	1 x DB-15, 2D Video Controller
	16MB Memory
Power	1+1 Redundant 750W Power Supply, Platinum level efficiency
Management interface	1 x 1GbE RJ-45, IPMI 2.0, RMM4 lite, Virtual media over LAN, KVM over LAN
LAN ports	Six (6) Intel I350 GbE connections
Storage devices	4x 960 GB SAS 12 Gb/s SSD, RAID 10
Cooling	6x40mm dual rotor managed system fans
	1+1 redundant 750 W power supply fan, Platinum level efficiency
	1800 BTU/hr is the approximate maximum heat dissipation under normal operation based on Ivanti EPMM's configuration.

M2600: front panel

The following figures, key, and LED table describe the M2600 font panel.

FIGURE 1. M2600 FRONT PANEL

M2600 front panel key:

A. Video port

B. USB ports

C. 960G Enterprise SSDs

D. NIC-2 Activity LED

E. Store drive activity LED

F. System ID button with LED

G. NMI button

H. NIC-1 activity LED

I. System cold reset button
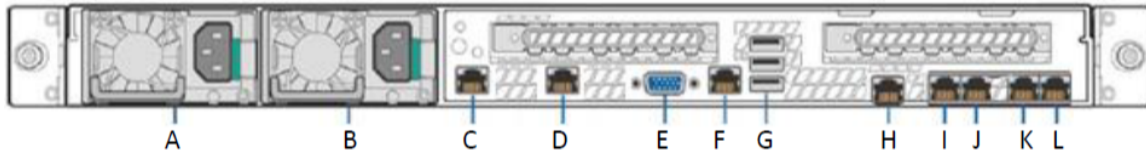
J. System status LED

K. Power button with LED

TABLE 35. INFORMATIONAL LED FIELDS

LED status	Description
Green	OK
Blinking green	Degraded - usually means a redundant part has failed.
Blinking amber	Degraded - System will fail soon
Solid amber	System failure

M2600: back panel

The following figure and key describe the M2600 back panel.

FIGURE 2. M2600 BACK PANEL

M2600 back panel key:

A. Power supply 1
B. Power supply 2
C. GigabitEthernet5
D. GigabitEthernet6
E. Video port
F. RJ45 serial port
G. USB ports
H. RMM4 NIC port
I. GigabitEthernet1
J. GigabitEthernet2
K. GigabitEthernet3
L. GigabitEthernet4

M2500 Series appliance

No new software releases are available for the Ivanti EPMM M2500 Series appliance. This version of Ivanti EPMM software has not been tested for compatibility with the M2500 Series appliance and is not supported.

M2250 Series appliance

The Ivanti EPMM appliance is a tightly integrated hardware, OS, application, and database solution that is built, optimized, and certified by Ivanti . The M2250 appliance ships with either Ivanti EPMM 10.1.0.0 or Ivanti Sentry 9.5 preinstalled. The following table lists the M2250 appliance specifications.

TABLE 36. IVANTI EPMM M2250 SERIES APPLIANCE SPECIFICATIONS

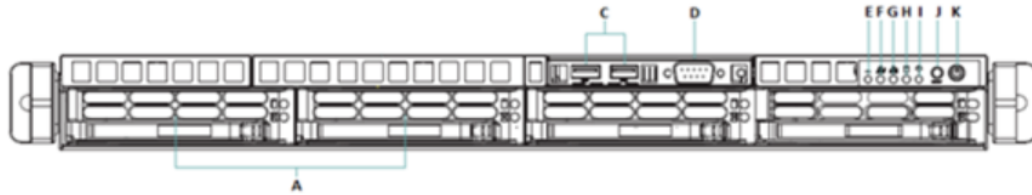|		
Operating environment	Processor	3.8 GHz Intel E3-1275 v6 CPU
	Memory	32 GB
	Drives	2 x 600 GB Hot-swap SAS3 12 GB/s SAS HW RAID
Chassis	Form Factor	19" 1U Rackmount
	Dimensions (D x H x W)	19.8" x 1.7" x 17.2" (503 mm x 43 mm x 437 mm)
	Weight	32 lbs (16.5 kg)
Front panel	Buttons	Power On/Off System Reset
	LEDs	Power LED Hard Drive Activity LED 2x Network Activity LED System Overheat LED
	USB	2x USB Ports
	Drives	600 GB Hot swap SAS 12.0 GB Hard Drives (RAID1) 1x Slim DVD Drive

TABLE 36. IVANTI EPMM M2250 SERIES APPLIANCE SPECIFICATIONS (CONT.)

Back panel	IPMI	Intelligent Platform Management Interface (IPMI) 2.0 with virtual media over LAN and KVM-over-LAN support; 1x 10/100BASE-T (RJ45)
	Ethernet	2x 10/100/1000BASE-T (RJ45)
	VGA	1x VGA (DB15)
	USB	4x USB Ports
	Serial	1x Serial port (DB9)
Power supply	Power	400W (1+1) Redundant Gold-level power supply with PMBus and I2C
	Voltage	100 – 240V, 50-60Hz, 6-3A +5V standby: 3A +12V: 33A +5V: 25A -12V: 0.6A
	Connector	IEC 60320-C13
Operating environment	Operating	Temperature: 50°F to 95°F (10°C to 35°C) Relative Humidity: 8% to 90% (non-condensing) Approximate maximum heat dissipation under normal operation based on Ivanti EPMM's configuration: 1262 BTU/hr
	Non-Operating	Temperature: -40° to 158°F (-40° to 70°C) Relative Humidity: 5% to 95% (non-condensing)

M2250: front panel

The following figure, key, and LED table describe the M2250 front panel.

FIGURE 1. M2250 FRONT PANEL

M2250 front panel key:

A. 600G HDDs
B. n/a
C. USB ports
D. Serial port
E. Informational LED
F. NIC-2 Activity LED
G. NIC-1 Activity LED
H. HDD Activity LED
I. Power LED
J. Reset button
K. Power button

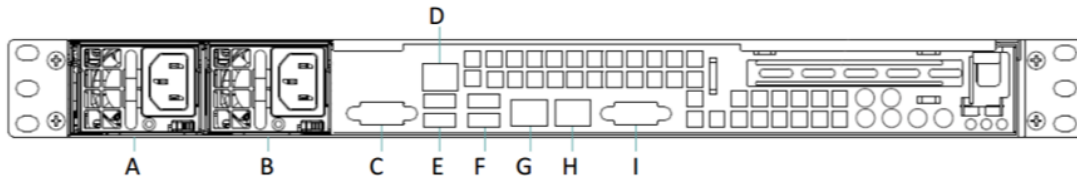TABLE 37. INFORMATIONAL LED FIELDS

LED status	Description
Solid red	An overheat condition has occurred. This may be caused by cable congestion.
Blinking red (1Hz)	A fan failure has occurred. Check for an inoperative fan.
Blinking red (0.25Hz)	A power failure has occurred. Check for a non-operational power supply
Solid blue	Location UID has been activated. Use this function to locate the server in a rack-mount environment.
Blinking blue (300 msec)	Remote UID is on. Use this function to identify the server from a remote location.

M2250: back panel

The following figure and key describe the M2250 back panel.
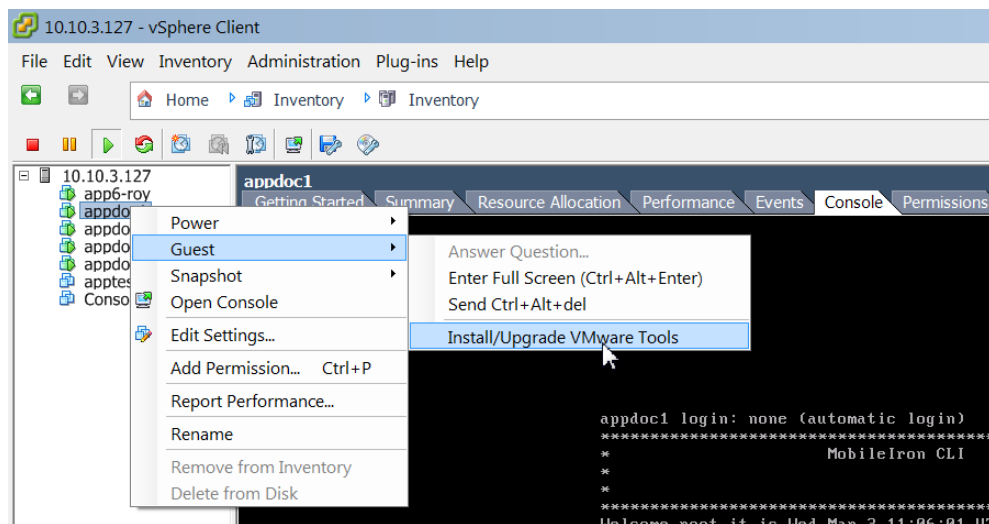
FIGURE 2. M2250 BACK PANEL

M2250 back panel key:

A. Power supply

B. Power supply

C. COM port

D. IPMI LAN

E. USB ports

F. USB ports

G. LAN1 port

H. LAN2 port

I. VGA port

VMware Tools setup

The Ivanti EPMM CLI includes a command that facilitates installation of VMware Tools.

1. In the vSphere Client, right-click the VM.

2. Select **Guest > Install/Upgrade VMware Tools**.

3. Enter the password.

4. Enter the following command: `#install rpm cdrom`

5. Select an rpm when prompted.

6. Enter the number for VMware Tools package.

7. Enter **enable**.

Outbound HTTP proxy set up

You can configure an outbound HTTP proxy for Ivanti EPMM. This proxy is intended primarily for organizations that require an HTTP proxy for communications with the Ivanti EPMM Gateway.

Procedure

1. In Admin Portal, select **Settings >System Settings > Security > Outbound HTTP**.

2. Use the following guidelines to complete the fields in this section:

Field	Description
HTTP Client Connect Timeout	Specify the amount of time to wait for the connection setup to complete.
HTTP Client Socket Timeout	Specify the amount of time to wait for a response from the proxy server.
HTTP Proxy URL	Enter the URL for the outbound HTTP proxy.
HTTP Proxy Auth Name	Enter the authentication name for the HTTP proxy.
HTTP Proxy Auth Password	Enter the authentication password for the HTTP proxy.

3. Click **Save**.

   At this point, the settings are saved, but not applied. To apply these changes, you need to reboot the entire system or enter the following commands using the CLI:

   ```
   enable
   service tomcat stop
   service tomcat start
   ```

The HTTP outbound proxy does not apply to the following areas:

- Ivanti EPMM client
- Sentry
- SCEP-to-CA connections