Integrate MDM and UEM Servers with Cisco ISE

Cisco Identity Services Engine
Updated September 3, 2026

© 2026 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

1 Integrate UEM and MDM Servers with Cisco ISE

Topics:

- Unified endpoint management in Cisco ISE
- MAC address for VPN-connected endpoints

Provides an introduction to endpoint management servers, such as Unified Endpoint Management (UEM) and Mobile Device Management (MDM) and how you can integrate them with Cisco ISE to enhance device management and security.

Unified endpoint management in Cisco ISE

Explains how you can integrate your Cisco ISE with endpoint management servers, Unified Endpoint Management (UEM) or Mobile Device Management (MDM), to access device attribute information from these servers through APIs.

If you secure, monitor, manage, and support network endpoints by using Unified Endpoint Management (UEM) or Mobile Device Management (MDM) servers, you can configure Cisco ISE to interoperate with these servers. Integrate Cisco ISE with your endpoint management servers to access device attribute information through APIs. To enable network access control, you can use the device attributes to create Access Control Lists (ACLs) and authorization policies.

Cisco ISE Policy Service Nodes (PSN) also use APIs to fetch lists of noncompliant devices from connected UEM or MDM servers at set polling intervals. Cisco ISE quarantines any noncompliant endpoints with active sessions at the time of polling and issues CoAs based on the fetched information.

You can configure your endpoint management servers to integrate them with Cisco ISE. Use the required configurations for your MDM or UEM vendor, such as

- Cisco Meraki Systems Manager
- Ivanti (previously MobileIron UEM) core and cloud UEM services
- Microsoft Endpoint Manager Intune

Cisco ISE also supports these endpoint management servers:

- 42Gears
- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Citrix XenMobile 10.x (On-prem)
- Globo
- IBM MaaS360
- Jamf Casper Suite
- Jamf Pro 10.42.0 or later
- Microsoft Endpoint Configuration Manager
- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- Omnissa (previously AirWatch)

After you configure the MDM or UEM servers to connect to Cisco ISE, join these servers to your Cisco ISE deployment. See "Configure Mobile Device Management Servers in Cisco ISE" in the chapter "Secure Access" in the *Cisco ISE Administrator Guide* for your release.

Cisco ISE MDM API version 3: Enhanced device identification with GUID

Cisco ISE MDM API version 3 enables device identification using a Globally Unique Identifier (GUID) instead of MAC addresses to uniquely identify devices, improving accuracy in deployments with randomized or changing MAC addresses. From Cisco ISE release 3.1, this enhancement enables more reliable network access control by using GUIDs provided by MDM servers instead of traditional device identifiers.

You can use Cisco ISE MDM API version 3 to receive a unique endpoint identifier, called GUID, from connected MDM and UEM servers. Cisco ISE then uses the GUID to identify an endpoint instead of its MAC address. Refer to "Handle Random and Changing MAC Addresses With Mobile Device Management Servers" in the chapter "Secure Access" in the *Cisco ISE Administrator Guide* for your release.

To receive GUID from a UEM or MDM server, these conditions must be met:

- The UEM or MDM server supports Cisco ISE MDM API version 3.
- Configure the certificates for Cisco ISE usage in your UEM or MDM so that the **Subject Alternative Name** field, the **Common Name** field, or both, push the GUID to Cisco ISE.

These UEM or MDM servers currently support Cisco ISE MDM API version 3:

- Cisco Meraki Systems Manager
- Ivanti (previously MobileIron UEM) core and cloud UEM services
- Microsoft Endpoint Manager Intune
- JAMF Casper Suite
- Omnissa (previously AirWatch)

For information on Omnissa configuration, refer to Omnissa Product Documentation.

MAC address for VPN-connected endpoints

Explains that VPN-connected endpoints share either their MAC address or UDID with Cisco ISE. Cisco ISE uses MAC addresses to manage endpoint data.

Cisco ISE uses endpoint MAC addresses to save and manage data, display context visibility information, and enable authorization workflows.

For VPN-connected endpoints, the VPN headend receives an endpoint's MAC address, Unique Device Identifier (UDID), or both from the Cisco Secure Client (formerly known as Cisco AnyConnect). It then sends the information to Cisco ISE over RADIUS communication.

When you integrate Cisco ISE with an MDM server, Cisco ISE uses either the endpoint's MAC address or the UDID to query the MDM server for the endpoint's registration, compliance status, and other MDM attributes.

When Cisco ISE queries an MDM server with endpoint's UDID, the MDM server usually responds with the endpoint's MAC address. Receiving an endpoint's MAC address from either the Cisco Secure Client or the MDM server is critical for Cisco ISE. Cisco ISE uses the MAC address to save and manage the endpoint data in its databases.

2 Integrate Cisco Meraki Systems Manager

Topics:

- Cisco Meraki Systems Manager
- Set up Cisco Meraki Systems Manager as an MDM or UEM server

Provides detailed instructions and configuration guidelines for setting up Cisco Meraki Systems Manager and integrating it with Cisco ISE for use as an MDM server.

Cisco Meraki Systems Manager

Introduces Cisco Meraki Systems Manager and explains how you can use it as an MDM server.

Cisco Meraki Systems Manager supports multiple platforms and helps manage diverse device ecosystems. Systems Manager offers centralized, cloud-based tools for endpoint management. Its scalable design supports growing organizations.

You can integrate Cisco Meraki Systems Manager as an MDM server in Cisco ISE. This allows you to use the endpoint information collected by Systems Manager for compliance checks and endpoint policy management.

For more information about Cisco Meraki Systems Manager, refer to the datasheet.

Cisco Meraki Systems Manager now supports MDM API version 3 and can provide Cisco ISE with a unique device identifier for connected endpoints.

Set up Cisco Meraki Systems Manager as an MDM or UEM server

Provides step-by-step instructions on how to connect Cisco Meraki Systems Manager to Cisco ISE for use as an MDM or UEM server.

To configure Cisco Meraki Systems Manager as an MDM or UEM server, follow this workflow:

1. Create a new profile.
2. Add SCEP certificate settings.
3. Configure Wi-Fi settings.
4. Apply and save Cisco ISE Wi-Fi profile on devices.
5. Configure organization MDM in Cisco Meraki Systems Manager.

Create a new profile

Learn how to create a new profile in Cisco Meraki Systems Manager.

Before you begin

In Cisco ISE, create and export a system certificate configured for administrator use.

To create and export a system certificate, refer to "System Certificates" in chapter "Basic Setup" in the *Cisco ISE Administrator Guide* for your release.

To create a new profile in Cisco Meraki Systems Manager, follow these steps:

Procedure

1. Log in to your Cisco Meraki Systems Manager portal.
2. From the main menu, go to **Systems Manager** > **Manage** > **Settings**.
3. Click **+ Add Profile**.
4. In the **Add New Profile** dialog box that appears, choose the **Device profile (Default)** radio button. Click **Continue**.
5. In the **Name** and **Description** fields, enter the required values.

Add SCEP certificate settings

Learn how to add SCEP certificate settings in Cisco Meraki Systems Manager.

To add Simple Certificate Enrollment Protocol (SCEP) certificate settings, perform these steps:

Procedure

1. Click **+Add** to add settings.
2. In the **Add New Settings Payload** window, click **SCEP Certificate**.
3. Perform these steps in the SCEP certificate window.
   a) In the **Name** field, enter a name for the SCEP certificate, such as ISE_SCEP.
   b) In the **Subject name** field, enter the common name value for the certificate.
   c) In the **Subject alternative name** field, enter **uri=ID:MerakiSM:DeviceID:$SM** Device ID. When you enter the dollar sign ($), a drop-down list of variables appears. Choose SM Device ID from the list.
   d) In the **Key Size** area, click the **2048** radio button.
   e) In the **Key Usage** area, check the **Signing** and **Encryption** check boxes.
   f) In the **CA Provider** area, choose a Certificate Authority (CA) provider from the drop-down list and click **Save**.

Configure Wi-Fi settings

Learn how to configure Wi-Fi settings in Cisco Meraki Systems Manager.

To configure Wi-Fi settings, perform these steps:

Procedure

1. Click **+Add settings** on the left side pane.
2. In the **Add New Settings Payload** window, click **Wi-Fi Settings**.
3. Enter the appropriate details in the Wi-Fi settings page.
   a) In the **SSID** field, enter the name of the Wi-Fi network to join.
   b) From the **Security** drop-down list, choose one of the Wi-Fi Protected Access (WPA) options.

      If you choose an enterprise option from the **Security** drop-down list, enter these details:

      - In the **Protocol** tab, check the check box of any certificate-based protocol, such as TLS.
      - In the **Authentication** tab, in the **Identity Certificate** area, from the drop-down list, choose the SCEP certificate that you created for the Cisco ISE use case.
      - In the Trust tab, in the **Trusted Certificates** area, check the check box next to the Cisco ISE certificate that you uploaded and click **Save**.

Apply and save Cisco ISE Wi-Fi profile on devices

Learn how to apply and save Cisco ISE Wi-Fi profile on devices.

To ensure the profile is assigned to the appropriate devices, perform these steps for applying tags and saving the profile:

Procedure

1. In the **Profile Configuration** tab, in the **Targets** area, add a tag for the Cisco ISE use case.

   For information on how to create and manage tags in Meraki Systems Manager, refer to Manage Tags. Applying tags ensures that the devices receive the relevant Cisco ISE profile with its certificate and Wi-Fi settings.

2. In the **You have unsaved changes** dialog box, click **Save**.

Provision organization MDM in Cisco Meraki Systems Manager

Learn how to configure organization MDM in Cisco Meraki Systems Manager.

To configure organization MDM in Cisco Meraki Systems Manager, perform these steps:

Procedure

1. In the left pane, navigate to **Organization > Configure > MDM**.
2. In the **Cisco ISE Settings** page:

   Make note of the username and password details you need to enter in Cisco ISE.

   To download the SCEP certificate, click **Download**.

What to do next

Connect Cisco Meraki Systems Manager as an MDM server in Cisco ISE. For information, refer to "Configure Mobile Device Management Servers in Cisco ISE" in the chapter "Secure Access" in the *Cisco ISE Administrator Guide* for your release.

3 Integrate Microsoft Endpoint Manager Intune

Topics:

- Microsoft Intune and Cisco ISE
- Configure Microsoft Endpoint Manager Intune
- Manage VPN-connected mobile devices with Microsoft Intune
- Connect Microsoft Intune to Cisco ISE as a mobile device management server

Provides detailed instructions and configuration guidelines for provisioning Microsoft Endpoint Manager Intune and integrating it with Cisco ISE for use as an MDM server.

Microsoft Intune and Cisco ISE

Introduces Microsoft Intune and explains that Cisco ISE supports integration with Microsoft Intune as an MDM solution.

Cisco ISE supports Microsoft Intune, an endpoint management solution, as an MDM integration. Communications between the two systems are governed by Microsoft's NAC integration designs as detailed in Network access control (NAC) integration with Intune.

Attention

From 2024-03-24, Microsoft no longer supports the Intune NAC service API for MAC address and UDID-based queries. Only the Microsoft Compliance Retrieval API (NAC 2.0 API) is supported, allowing both GUID and MAC address-based queries, starting 2023-07-31.

After 2024-03-24, you must upgrade to one of these Cisco ISE releases to continue using your Microsoft Intune integrations:

- Cisco ISE release 3.1 patch 8
- Cisco ISE release 3.2 patch 4

The earlier patches of these releases cannot retrieve device registration and compliance information from connected Microsoft Intune servers from March 24, 2024.

With Microsoft's NAC 2.0 API, Cisco ISE can only retrieve these endpoint attribute information:

- Compliance status
- Managed by Intune
- MAC address
- Registered status

Configure Microsoft Endpoint Manager Intune

Provides step-by-step instructions on how to connect Microsoft Endpoint Manager Intune with Cisco ISE, and enable Cisco ISE MDM API v3 support to receive GUID from Microsoft Intune.

These steps list the configurations to carry out in Microsoft Endpoint Manager Intune.

- Choose the steps that your organization needs.
- If you use Cisco ISE release 3.1 or a later release, you can enable Cisco ISE MDM API v3 support to receive GUID from Microsoft Intune.

  To enable this support, configure the Subject Alternative Name (SAN) in your certificate profiles. Configuring the SAN allows Cisco ISE to receive a unique GUID for an endpoint from the Intune server. This helps address issues caused by random and changing MAC addresses.
- If your organization does not use the standard commercial Microsoft Azure environment, refer to the Microsoft National Cloud Deployments document for a list of Graph API endpoints for national clouds operated by Microsoft.

.

Procedure

1. Configure certificates for endpoint authentication in Microsoft Intune.
2. Configure either SCEP or PKI certificate management protocols and the appropriate certificate profiles, according to your organizational needs.

   For SCEP:

   a. Configure infrastructure to support SCEP with Microsoft Intune.

   b. Create and assign SCEP certificate profiles in Microsoft Intune.

   For private and public key infrastructure (PKI):

   a. Configure and use PKCS certificates with Microsoft Intune.

   b. Create a PKCS certificate profile.

   > **Tip**
   >
   > When you configure an SCEP or a PKI profile, in the **Subject Alternative Name** page, choose **URI** as the **Attribute**, and **ID:Intune:GUID:{{DeviceId}}** as the **Value**.
   >
   > The **ID:Intune:GUID:{{DeviceId}}** is a template for reference.

3. For Wi-Fi and wired endpoints, create a profile and choose the SCEP or PKI certificate profile you configured earlier to include the GUID value in the **Subject Alternative Name** field.

   For more details on configuring Wi-Fi settings in Microsoft Intune, refer to Add and use Wi-Fi settings on your devices in Microsoft Intune.

   If you create VPN profiles to connect to VPN servers in Intune, you must choose the certificate-based authentication type to share the GUID value with Cisco ISE.

Manage VPN-connected mobile devices with Microsoft Intune

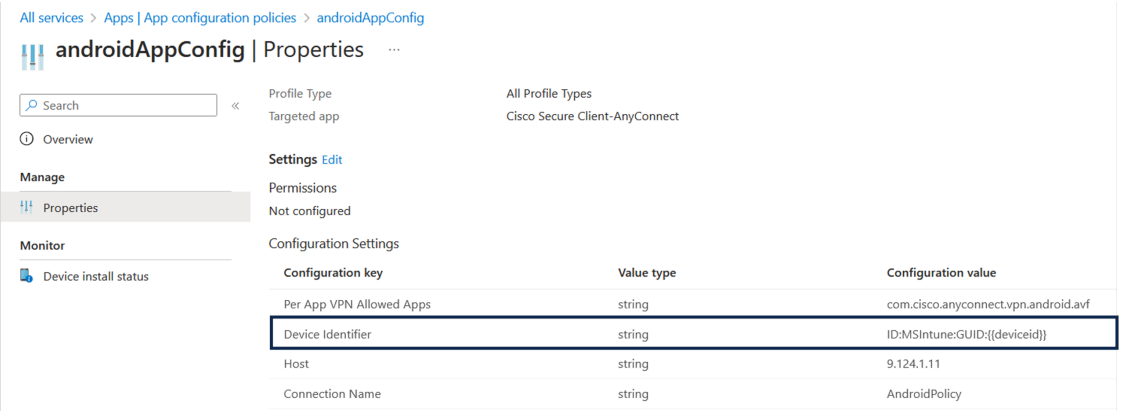
Describes how to use Microsoft Intune to manage mobile devices connected by VPN.

To manage VPN-connected mobile devices, these configurations are required in Microsoft Intune:

VPN-connected android device settings in Microsoft Intune

1. Configure settings for VPN-connected Android endpoints according to the requirements detailed in Android enterprise device settings to configure VPN in Intune.
2. Create an app configuration policy in Microsoft Intune for endpoints that use the Cisco Secure Client-AnyConnect app. Include the **Device Identifier** configuration key in the Configuration Settings for this policy.

   Figure 1: App configuration policy settings in Microsoft Intune



VPN-connected iOS device settings in Microsoft Intune

For VPN-connected iOS devices, you can find the required VPN settings for Microsoft Intune in Add VPN settings on iOS and iPad OS devices in Microsoft Intune.

Restriction

When you create a VPN profile for iOS or iPadOS devices, you must choose the **Enable network access control (NAC)** setting to allow Microsoft Intune to include a device ID for the endpoint.

After you complete these configurations, Cisco AnyConnect logs the device identifier in the format **ID:Intune:DeviceID:<*device id*>**. Cisco ISE APIs retrieve this device ID for the endpoint. The system uses the device ID instead of the endpoint's MAC address to check compliance.

Connect Microsoft Intune to Cisco ISE as a mobile device management server

Provides step-by-step instructions on how to connect Microsoft Intune to Cisco ISE as an MDM server.

Microsoft Intune retired support for Azure AD Graph Applications on June 30, 2023. You must migrate any integrations that use Azure AD Graph to Microsoft Graph. Cisco ISE typically uses the Azure AD Graph for integration with the endpoint management solution Microsoft Intune.

To configure Microsoft Intune as an MDM or UEM server, follow this workflow:

1. Register account.
2. Export Cisco ISE certificate.
3. Upload Cisco ISE certificate to Microsoft Azure.
4. Set API permissions and collect application details.
5. Download and import Microsoft Intune certificates into Cisco ISE.
6. Add Microsoft Intune as an external MDM server.
7. Manage MDM server status in Microsoft Intune.

Register Account

Learn how to register your account to start integrating Microsoft Intune to Cisco ISE as an MDM server.

Follow these steps to register your account to start integrating Microsoft Intune to Cisco ISE as an MDM server.

Before you begin

You must upgrade to one of these Cisco ISE releases that support Microsoft Graph applications for successful integration with Microsoft Intune:

- Cisco ISE release 3.1 patch 3 and later releases
- Cisco ISE release 3.2 and later releases

For more information on the migration from Azure AD Graph to Microsoft Graph, refer to these resources:

- Migrate Azure AD Graph apps to Microsoft Graph
- Azure AD Graph to Microsoft Graph migration FAQ
- Update your applications to use Microsoft Authentication Library and Microsoft Graph API

After you update Cisco ISE to one of the supported versions, in each Microsoft Intune server integration in Cisco ISE, manually update the **Auto Discovery URL**.

Replace **https://graph.windows.net*<Directory (tenant) ID>*** with **https://graph.microsoft.com**.

Procedure

1. Log in to the Microsoft Azure portal, and navigate to **Azure Active Directory**.
2. Choose **Manage** > **App registrations**.
3. Click **New registration**.
4. In the **Register an application** page, enter a value in the **Name** field.
5. In the **Supported Account Types** area, click the **Accounts in this organizational directory only** radio button.
6. Click **Register**.

   The **Overview** window of the newly registered application is displayed. With this window open, log in to the Cisco ISE administration portal.

Export Cisco ISE certificate

Learn how to export a Cisco ISE certificate.

Follow these steps to export a Cisco ISE certificate.

Procedure

1. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System** > **Certificates**.
2. From the list of certificates, check the check box next to the **Default self-signed server certificate**, or next to any other certificate you have configured for **Admin** usage, and click **Export**.
3. In the dialog box displayed, click the **Export Certificate Only** radio button, then click **Export**.
4. Click **View** to see the details of this certificate. Scroll down the displayed **Certificate Hierarchy** dialog box to the **Fingerprints** area and note the values.

Upload Cisco ISE certificate to Microsoft Azure

Learn how to upload a Cisco ISE certificate to Microsoft Azure.

Follow these steps to upload a Cisco ISE certificate to Microsoft Azure.

Procedure

1. In the Microsoft Azure Active Directory portal, click **Certificates and Secrets** in the left pane.
2. Click **Upload certificate** and upload the exported Cisco ISE certificate.

   Remember

   If there is any change in the status of the Cisco ISE self-signed certificate, you must perform the Manage MDM server status in Microsoft Intune on page 19 procedure in Cisco ISE.

3. After the certificate is uploaded, verify that the **Thumbprint** value matches the **Fingerprint** value in the Cisco ISE certificate.
4. Navigate to **Manifest** on the left pane.

   Confirm that the **displayName** value matches the common name in the Cisco ISE certificate.

Set API permissions and collect application details

Learn how to set API permissions and collect application details.

Follow these steps to set API permissions and collect application details.

Procedure

1. In the Microsoft Azure portal, click **API permissions**.
2. Click **Add a permission** and add these permissions:

API or permission name	Type	Description
Intune		
get_device_compliance	Application	Obtain device state and compliance information from Microsoft Intune.
Microsoft Graph		
Application.Read.All	Application	Read all applications.

3. Click **Grant admin consent for** > ***tenant name***.

   Note the **Application (client) ID** and the **Directory (tenant) ID** from the **Overview** page of the application.
4. Click **Endpoints** in the **Overview** page. Note the value in the **Oauth 2.0 token endpoint (V2)** field.

Download and import Microsoft Intune certificates into Cisco ISE

Learn how to download and import Microsoft Intune certificates into Cisco ISE.

Follow these steps to download and import Microsoft Intune certificates into Cisco ISE.

Procedure

1. Download the Microsoft Intune certificates from DigiCert Root Certificates in the PEM certificate (chain) format.

   If you see the error "Connection Failed to the MDM server: There is a problem with the server Certificates or Cisco ISE trust store,". This message indicates that the Cisco ISE does not trust the Microsoft Intune certificates. To resolve this issue, capture network traffic on the Cisco ISE Primary Administration Node (PAN) to identify the certificates used by Microsoft. Download the certificates from the Microsoft PKI repository and import them into Cisco ISE's Trusted Certificates store. After you update, disable the MDM server status in Cisco ISE and then re-enable it to refresh the connection and restore trust.

   > **Tip**
   >
   > To ensure a successful connection between Microsoft Intune and Cisco ISE, import new root certificates. For more information, refer to Intune certificate updates: Action may be required for continued connectivity.

2. In the Cisco ISE administration portal, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**.
3. For each downloaded certificate:
   a. Click **Import**.
   b. Click **Choose File** and choose the corresponding downloaded certificate from your system.
   c. In the **Usage** area, check the **Trust for authentication within Cisco ISE** and **Trust for authentication of Cisco Services** check boxes.
   d. Click **Save**.

Add Microsoft Intune as an external MDM server

Learn how to add Microsoft Intune as an external MDM server.

Follow these steps to add Microsoft Intune as an external MDM server.

Procedure

1. In the Cisco ISE administration portal, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **External MDM**.
2. Click **Add** and enter a value in the **Name** field.
3. From the **Authentication Type** drop-down list, choose **OAuth – Client Credentials**.
4. Enter these details in the respective fields:
   - **Auto Discovery URL**: https://graph.microsoft.com.

Remember

The URL **https://graph.windows.net<Directory*(tenant) ID*>** was used when Microsoft Intune supported Azure AD Graph Applications. However, Microsoft Intune retired support for Azure AD Graph Applications on 2023-06-30. Upgrade to a Cisco ISE release that supports Microsoft Graph for successful integration.

These are the Cisco ISE releases that support Microsoft Graph applications:

- Cisco ISE release 3.1 patch 3 and later
- Cisco ISE release 3.2 and later releases

- **Client ID**: Enter the **Application (client) ID** value from the Microsoft Intune application.
- **Token Issuing URL**: Enter the **Oauth 2.0 Token Endpoint (V2)** value.
- **Token Audience**: Enter **https://api.manage.microsoft.com//.default** if you use these releases of Cisco ISE:
  - Cisco ISE release 3.1 patch 8 and later releases
  - Cisco ISE release 3.2 patch 3 and later releases, and
  - Cisco ISE release 3.3 and later releases

  Important

  In the listed Cisco ISE releases, when you create a new integration, the new token audience value is automatically filled when you choose **OAuth–Client Credentials**. If you upgrade to these releases with existing integrations, you must update the token audience field manually to continue receiving updates from the integrated servers.

  This is because Microsoft mandates that applications that use the Azure Active Directory Authentication Library (ADAL) for authentication and authorization must migrate to the Microsoft Authentication Library (MSAL). For more information, refer to Migrate applications to the Microsoft Authentication Library (MSAL).

  For other releases of Cisco ISE, enter **https://api.manage.microsoft.com/**.

Important

Microsoft Intune dynamically redirects API requests to regional Front-End Forwarder (FEF) endpoints under `*.manage.microsoft.com`, based on the tenant's geographic location and Azure datacenter routing. If your firewall supports domain-based rules, use `*.manage.microsoft.com` and `manage.microsoft.com`. Otherwise, use the approved list of subnets in this section.

5. Enter the required values for the **Polling Interval** and **Time Interval For Compliance Device ReAuth Query** fields.
6. Click **Test Connection** to ensure that Cisco ISE can connect to the Microsoft server.
7. When the connection test is successful, choose **Enabled** from the **Status** drop-down list and click **Save**.

In the Cisco ISE administration portal, click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **External MDM**. The Microsoft Intune server that is added must be displayed in the list of **MDM Servers** displayed.

Manage MDM server status in Microsoft Intune

Learn how to manage MDM server status in Microsoft Intune.

After uploading a new certificate to Microsoft Intune, first disable the MDM server status, then re enable it.

Follow these steps to manage MDM server status in Microsoft Intune.

Procedure

1. Click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **External MDM**.
2. Click **Edit**.
3. Click **Test Connection** to ensure that Cisco ISE can connect to the Microsoft server.
4. When the connection test succeeds, choose **Disabled** from the **Status** drop-down list and click **Save**.
5. Click **Edit**, then click **Test Connection** .
6. When the connection test succeeds, choose **Enabled** from the **Status** drop-down list and click **Save**.

4 Integrate Ivanti (previously MobileIron) UEM

Topics:

- Ivanti (previously MobileIron) UEM servers
- Set up MobileIron Cloud UEM servers
- Set up MobileIron Core UEM servers

Provides detailed instructions and configuration guidelines for deploying Ivanti (previously MobileIron) UEM and integrating it with Cisco ISE for use as a UEM server.

Ivanti (previously MobileIron) UEM servers

Introduces Ivanti (previously MobileIron) and describes how to connect Ivanti UEM servers to Cisco ISE.

Attention

MobileIron is now part of Ivanti. At the time of writing, MobileIron continues to offer Unified Endpoint Management (UEM) solutions such as MobileIron Core (On-Premises) and MobileIron Cloud.

Cisco ISE release 3.1 leverages APIs through the BasicAuth framework to connect to MobileIron Core or MobileIron Cloud servers. It receives GUID values from these servers. Cisco ISE uses these GUID values instead of MAC addresses to identify endpoints. This process enables reliable authentication even when MAC Address Randomization is in use.

GUID-based authentication uses client certificates, also called X509 or Identity Certificates. To ensure certificates sent from MobileIron Cloud or MobileIron Core servers to Cisco ISE include GUID values, complete these tasks:

Configuration steps in Ivanti

To use GUID with Cisco ISE, ensure you have MobileIron Core 11.3.0.0 Build 24 or later.

In the MobileIron Cloud or MobileIron Core administrator portal:

1. Create a user account and assign the required API permissions to it.
2. Configure a Certificate Authority (CA).
3. Configure an Identity Certificate to include GUID information.
4. Upload root certificates or trusted certificates, as required.
5. Configure a Wi-Fi profile.

Tip

- If you have already connected MobileIron Cloud or MobileIron Core servers to your Cisco ISE release 3.1 and want to receive GUIDs from the connected servers, perform steps 3, 4, and 5, as required.
- When you edit your existing Identity Certificate or Wi-Fi configurations, or both, MobileIron republishes the updated configurations to your managed devices that are connected.
- Although MobileIron does not recommend using self-signed certificates or a local CA, this guide includes the steps for self-signed certificates and a local CA as an example to highlight the Subject and Subject Alternative Name attribute configurations necessary for handling random and changing MAC addresses in Cisco ISE release 3.1.

Configuration steps in Cisco ISE

In Cisco ISE:

1. Upload the certificate generated in the MobileIron portal.
2. Connect the MobileIron UEM servers.

Set up MobileIron Cloud UEM servers

Provides step-by-step instructions on how to configure MobileIron Cloud UEM servers.

To configure MobileIron Cloud UEM server, follow this workflow.

1. Add MobileIron Cloud user for Cisco ISE operations.
2. Configure a certificate authority in MobileIron Cloud.
3. Upload root or trusted certificates in MobileIron Cloud.
4. Configure an identity certificate in MobileIron Cloud.
5. Configure a Wi-Fi profile in MobileIron Cloud.

Add MobileIron Cloud user for Cisco ISE operations

Learn how to add a MobileIron Cloud user account and assign the Cisco ISE operations role.

Follow these steps to add a MobileIron Cloud user account and assign the Cisco ISE operations role.

Procedure

1. Log in to the MobileIron Cloud portal.
2. From the top menu, choose **Users**.
3. From the **Add** drop-down list, choose **Add API User**.
4. In the **Add API User** window, enter values for these fields:
   - **Username**
   - **Email Address**
   - **First Name**
   - **Last Name**
   - **Password**
   - **Confirm Password**
5. In the **Assign Roles** area, check the **Cisco ISE Operations** check box to allow the user to invoke the APIs required for Cisco ISE integration.
6. Click **Done**.

Establish a certificate authority in MobileIron Cloud

Learn how to configure a local certificate authority (CA) in MobileIron Cloud.

MobileIron Cloud also offers a wider range of certificate authority (CA) configurations. Choose the type that best matches your organization's requirements.

For information on the various types of certificate management supported by MobileIron Cloud, refer to http://mi.extendedhelp.mobileiron.com/75/all/en/Welcome.htm#LocalCertificates.htm.

Follow these steps to configure a local certificate authority (CA) in MobileIron Cloud.

Procedure

1. In the MobileIron Cloud portal, choose **Admin** > **Certificate Management**.
2. Click **Add**.
3. Click **Create a Standalone Certificate Authority**.
4. In the dialog box , enter the details in the respective fields.
   a. **Name**
   b. In the **Subject Parameters** area, enter a value for at least one of these fields:
      - **Common Name**
      - **Email**
      - **Organization Unit**
      - **Organization**
      - **Street Address**
      - **City**
      - **Region**
      - **Country**
   c. In the **Key Generation Parameters** area:
      - From the **Key Type** drop-down list, choose **RSA**.
      - From the **Signature Algorithm** drop-down list, choose **SHA256withRSA**.
      - From the **Key Length** drop-down list, choose **2048**.

Upload root or trusted certificates in MobileIron Cloud

If you do not use trusted third-party CAs, upload root or trusted certificates in MobileIron Cloud.

If you use a trusted third-party CA to generate identity certificates, you can ignore this task.

If you use the local MobileIron Cloud CA or an internal CA that is private to your company or organization, you must upload the Root Certificate of the CA. When you upload this certificate, it is distributed to the connected devices, which can then trust the source or issuer of the identity certificate used for authentication.

Follow these steps to upload root or trusted certificates in MobileIron Cloud.

Procedure

1. From the MobileIron Cloud menu, choose **Configurations**.
2. Click **Add** and choose **Certificate**.
3. In the **Name** field, enter a name for the trusted certificate.
4. In the **Configuration Setup** area, click **Choose File** and choose the trusted or root certificate for your CA.
5. Click **Next**.

Create an identity certificate in MobileIron Cloud

Learn how to create an identity certificate in MobileIron Cloud.

Configure an identity certificate in MobileIron Cloud to set up the certificate authentication mechanism for mobile devices. Identity Certificates are X.509 certificates (.p12 or .pfx files). You can also generate identity certificates dynamically using a CA as the source.

> **Tip**
>
> If you have identity certificates in MobileIron cloud that are already configured for Cisco ISE MDM use cases, update the certificate's settings to enable GUID information retrieval from MobileIron servers.

Follow these steps to create an identity certificate in MobileIron Cloud.

Procedure

1. From the MobileIron Cloud top menu, choose **Configurations** and click **Identity Certificate**.
2. In the **Name** field, enter a value.
3. In the **Configuration Setup** area, from the drop-down list, choose **Dynamically Generated**.
4. From the **Source** drop-down list, choose the CA that you configured in the procedure Configure a Certificate Authority in MobileIron Cloud.
5. From the **Subject Alternative Name Type** drop-down list, choose **Uniform Resource Identifier**.
6. In the **Subject Alternative Name Value** field, enter **ID:Mobileiron:GUID:${deviceGUID}**. Configure the Subject Alternative Name field for GUID.

   Optional: Alternatively, to use the Common Name (CN) field to push GUID to Cisco ISE, in the **Subject** field, enter **CN=ID:Mobileiron:GUID:${deviceGUID}**.
7. Click **Test Configuration and Continue**.
   The **Configuration Test Successful** dialog box displays the details of the created identity certificate.
8. In the **Distribute** window, click **Custom**.
9. In the **Define Device Group Distribution** area, choose the device groups that you want to distribute in this configuration and click **Done**.

   If you update the SAN or CN fields in an existing identity certificate for Cisco ISE MDM use cases, the updated certificates must be sent to the end users connected to your network.

   To send the updated certificates to end users, in the **Configurations** > **Choose Config** > **Edit** window, check the **Clear cached certificates and issue new ones with recent updates** check box.

Define a Wi-Fi profile in MobileIron Cloud

Learn how to configure a WiFi profile in MobileIron Cloud.

If you have already deployed Wi-Fi profiles to your managed iOS and Android devices, edit the Wi-Fi profiles to include the latest identity certificate configuration. The connected devices will then receive new identity certificates with a GUID in the **Subject** or **Subject Alternative Name** attributes.

Follow these steps to configure a WiFi profile in MobileIron Cloud.

Procedure

1. From the MobileIron Cloud menu, choose **Configurations** and click **Wi-Fi**.
2. In the **Name** field, enter a value.
3. In the **Service Set Identifier (SSID)** field, enter the name of your network.

   Note

   The **Auto Join** check box is checked by default. Keep the default selection.

4. From the **Security Type** drop-down list, choose the required option.
5. In the **Enterprise Settings** area, in the **Protocols** tab, check the **TLS** check box.
6. In the **Authentication** tab, enter the required values in the **Username** and **Password** fields.
7. From the **Identity Certificate** drop-down list, choose the identity certificate that you created in the procedure Create an identity certificate in MobileIron Cloud on page 25.

   Optional: In the **Trust** tab, check the check box adjacent to the trusted certificate that you want to use.
8. In the **All Versions** area, from the **Network Type** drop-down list, choose **Standard** and click **Next**.

   In the **Distribute** window, click the required option.
9. In the **Define Device Group Distribution** area, check the check boxes adjacent to the device groups that you want to include in this configuration and click **Done**.

Set up MobileIron Core UEM servers

Provides step-by-step instructions on how to configure MobileIron Core UEM servers.

To configure MobileIron Core UEM server, follow this workflow.

1. Add a MobileIron Core user with API permissions on page 26.
2. Configure a certificate authority in MobileIron Core.
3. Add root or trusted certificates in MobileIron Core.
4. Configure certificate enrollment in MobileIron Core.
5. Configure a Wi-Fi profile in MobileIron Core.
6. Map resources to labels in MobileIron Core.

Add a MobileIron Core user with API permissions

Learn how to create a MobileIron Core user and assign API permissions.

Follow these steps to create a MobileIron Core user and assign API permissions.

Procedure

1. Log in to your MobileIron Core administrator portal.

2. Choose **Devices and Users** > **Users**.
3. From the **Add** drop-down list, choose **Add Local User**.
4. Enter the required values in these fields:
   - **User ID**
   - **First Name**
   - **Last Name**
   - **Password**
   - **Confirm Password**
   - **Email**
5. Click **Save**.
6. To assign an API role to the newly created user, click **Admin** and check the check box next to the corresponding user name.
7. From the **Actions** drop-down list, choose **Assign to Space**.
8. Choose a predefined space for the user from the **Select Space** drop-down list, or choose the roles that you want to assign to the user from the available options. Ensure that the user has tenant administrator permissions and that the **API role** is enabled for this user.
9. Click **Save**.

Establish a certificate authority in MobileIron Core

Learn how to add a CA to MobileIron Core.

MobileIron Core allows you to choose from a wider range of certificate authority (CA) configurations. Choose the option that suits your organization's requirements.

Follow these steps to add a certificate authority (CA) to MobileIron Core. This procedure includes steps for creating self-signed certificates only as an example.

Procedure

1. In the MobileIron Core administrator portal, choose **Services** > **Local CA**.
2. From the **Add** drop-down list, choose **Generate Self-Signed Cert**.
3. In the **Generate Self-Signed Certificate** dialog box that is displayed, enter the required values in each fields:
   - **Local CA Name**
   - **Key Length**
   - **CSR Signature Algorithm**
   - **Key Lifetime (in days)**
   - **Issuer Name**
4. Click **Generate**.
5. Download the CA certificate. Later, you will upload this certificate to Cisco ISE. Click **View Certificate** next to the certificate that you want to download. Copy all the contents into the displayed dialog box. Paste the certificate content into a text editor and save the document as a .cer file.

Add root or trusted certificates in MobileIron Core

Learn how to upload root and trusted certificates in MobileIron Core.

Follow these steps to upload root and trusted certificates in MobileIron Core.

Procedure

1. In the MobileIron Core administrator portal, choose **Policies and Configs** > **Configurations**.
2. From the **Add New** drop-down list, choose **Certificates**.
3. In the **New Certificate Setting** dialog box, enter name and description for the certificate in the corresponding fields.
4. In the **File Name** page, click **Browse**. Choose the root or trusted certificate you need to upload for the CA you configured.

   The accepted file types are certificate files with extensions .cer, .crt, .pem, and .der.
5. Click **Save**.

Provision certificate enrollment in MobileIron Core

Learn how to connect a CA and configure **Subject** and **SAN** fields to capture GUID and handle random and changing MAC addresses.

This procedure highlights the **Subject** and **Subject Alternative Name** attribute configurations needed to handle random and changing MAC addresses in Cisco ISE release 3.1. MobileIron does not recommend the use of self-signed certificates or a local CA.

Follow these steps to connect a CA and configure **Subject** and **SAN** fields to capture GUID and handle random and changing MAC addresses.

Procedure

1. In the MobileIron Core administrator portal, choose **Policies and Configs** > **Configurations**.
2. Click **Add New**, choose **Certificate Enrollment** and then choose the appropriate connector for the CA you have configured. If you are configuring a local CA, Choose **Local**.

   This procedure explains how to configure local CA. Choose the certificate enrollment option that matches the CA you have configured to connect your MobileIron Core servers to Cisco ISE.
3. In the **New Local Certificate Enrollment Setting** dialog box that is displayed, provide values for these fields:
   - **Name**
   - **Local CAs**
   - **Key Type**
   - **Subject**: To use the **Subject** field to share the UUID (referred to as GUID in Cisco ISE) with Cisco ISE release 3.1 and later, enter **CN=ID:Mobileiron:GUID:${deviceGUID}**.
   - **Key Length**
   - **CSR Signature Algorithm**

- In the **Subject Alternative Names** area, click **Add** and choose **Uniform Resource Identifier** from the **Type** drop-down list. In the **Value** column, enter **ID:Mobileiron:GUID:${deviceGUID}**. This field shares the UUID (referred to as GUID in Cisco ISE) with Cisco ISE release 3.1 and later.

4. Click **Issue Test Certificate**.

Define a Wi-Fi profile in MobileIron Core

Learn how to configure a WiFi profile in MobileIron Core.

Follow these steps to configure a WiFi profile in MobileIron Core.

Procedure

1. In the MobileIron Core administrator portal, choose **Policies and Configs** > **Configurations**.
2. From the **Add New** drop-down list, choose **Wi-Fi**.
3. In the **New Wi-Fi Setting** dialog box, enter the required values in these fields:
   - In the **EAP Type** area, check the **TLS** check box.
   - From the **Identity Certificate** drop-down list, choose the certificate enrollment that you configured in the procedure Provision certificate enrollment in MobileIron Core on page 28.
   - Click **Save**.

Map resources to labels in MobileIron Core

Learn how to configure a label in MobileIron Core to define the configurations, rules, and profiles that must be applied to a group of endpoints and devices.

Configure a label to define the configurations, rules, and profiles for a group of endpoints and devices. You can use a label to group endpoints and devices by criteria such as organizational unit, device type, or operating system that are running on an endpoint. After you create a label, assign it to resources in the **Policies & Configs** page to map configurations, policies, and device or user groups.

To support the Cisco ISE use case, first create an appropriate label. Then apply the certificate enrollment, Wi-Fi profile, and other configurations you create for this use case to that label.

Follow these steps to configure a label in MobileIron Core to define the configurations, rules, and profiles that must be applied to a group of endpoints and devices.

Procedure

1. Create a label:
   a. In the MobileIron Core administrator portal, choose **Devices & Users** > **Labels**.
   b. Click **Add Label**.
   c. In the **Add Label** dialog box, enter a name for the label in the **Name** field.
   d. In the **Criteria** area, define the parameters of this label by choosing the appropriate values in the **Field**, **Operator**, and **Value** fields.
   e. Click **Save**.

2. Assign a label to a **Policies & Configs** resource:
   a. In the MobileIron Core administrator portal, click **Policies & Configs** and choose the resource menu of your choice.
   b. Check the check box for the configuration or policy to which you want to assign the label that you created.
   c. From the **Actions** drop-down list, choose **Apply To Label**.
   d. In the **Apply To Label** dialog box, check the check box adjacent to the label that you want to apply, and click **Apply**.

© 2026 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)