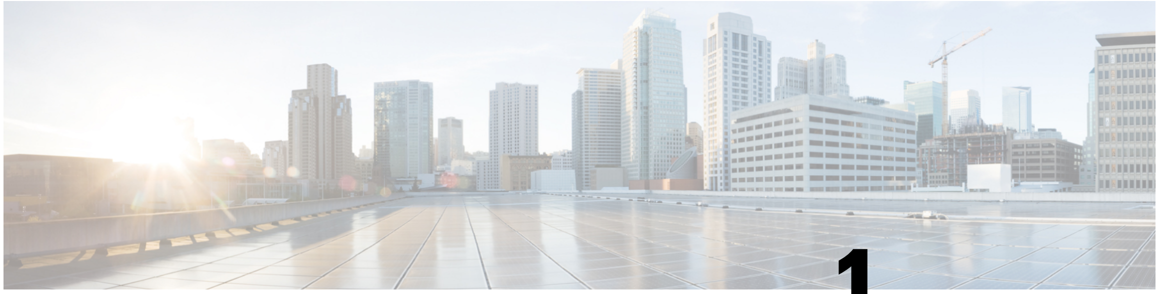
Integrate MDM and UEM Servers with Cisco ISE

First Published: 2020-08-16

Last Modified: 2024-03-26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Integrate UEM and MDM Servers With Cisco ISE

- Overview of Unified Endpoint Management in Cisco ISE, on page 1
- MAC Address for VPN-Connected Endpoints, on page 3
- Additional References, on page 3
- Communications, Services, and Additional Information, on page 3

Overview of Unified Endpoint Management in Cisco ISE

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

Cisco ISE PSNs also send APIs to fetch lists of noncompliant devices from connected UEM or MDM servers at set polling intervals. Any noncompliant endpoints with active sessions at the time of polling are quarantined and CoAs are issued in Cisco ISE based on the fetched information.

This document details the configurations that you must perform in your endpoint management servers to integrate these servers with Cisco ISE. This document currently details the required configurations for the following MDM or UEM vendors:

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

Cisco ISE also supports the following endpoint management servers:

- 42Gears
- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Citrix XenMobile 10.x (On-prem)
- Globo

- IBM MaaS360
- JAMF Casper Suite
- Microsoft Endpoint Configuration Manager
- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE (previously AirWatch)

Note Cisco ISE 3.0 or earlier releases cannot be integrated with Jamf Pro 10.42.0 or later.

After you carry out the necessary configurations in the MDM or UEM servers that you want to connect to Cisco ISE, you must join the servers to your Cisco ISE. 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 for GUID

Cisco ISE Release 3.1 introduces the capability to handle random and changing MAC addresses of endpoints. You can use Cisco ISE MDM API Version 3 to receive a unique endpoint identifier that is named GUID from the connected MDM and UEM servers. Then, Cisco ISE uses the GUID to identify an endpoint instead of its MAC address. See "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, the following conditions must be met:

- The UEM or MDM server supports Cisco ISE MDM API Version 3.
- In the UEM or MDM, the certificates for Cisco ISE usage are configured so that the Subject Alternative Name field, or the Common Name field, or both, push the GUID to Cisco ISE.

The following 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
- VMware Workspace ONE (previously AirWatch)

Note For information on VMware Workspace ONE configuration, see

MAC Address for VPN-Connected Endpoints

Cisco ISE uses the MAC addresses of endpoints to save and manage endpoint data in its databases, display context visibility information, and enable authorization workflows.

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

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

If Cisco ISE queries an MDM server using an endpoint's UDID, the compliance response from the MDM server usually includes 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.

Additional References

See Cisco ISE End-User Resources for additional resources that you can use when working with Cisco ISE.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

CHAPTER 2

Integrate Cisco Meraki Systems Manager

- Configure Cisco Meraki Systems Manager , on page 5

Configure Cisco Meraki Systems Manager

Cisco Meraki Systems Manager supports a variety of platforms, enabling the diverse device ecosystems that are commonplace today. Systems Manager offers centralized, cloud-based tools for endpoint management with far-reaching scalability for growing organizations. Integrate Cisco Meraki Systems Manager as an MDM server in Cisco ISE to leverage the endpoint information that is collected by Cisco Meraki Systems Manager for compliance checks and endpoint policy management.

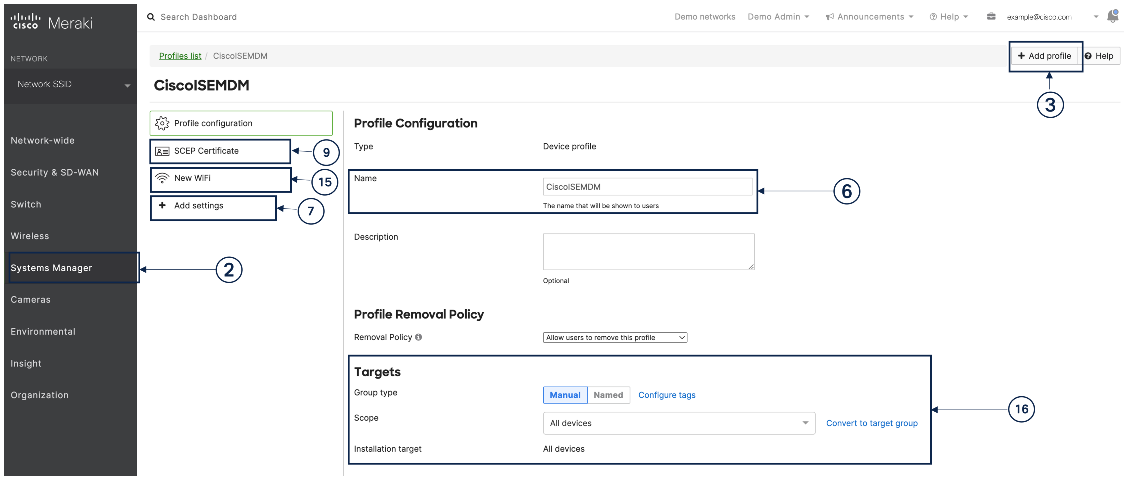
For more information about Cisco Meraki Systems Manager, see the datasheet.

Cisco Meraki Systems Manager now supports MDM API version 3 and can provide Cisco ISE with a unique device identifier for connected endpoints. If you already have an active Cisco Meraki Systems Manager integration in your Cisco ISE, carry out Steps 8 to 15 for the Cisco ISE-related device profile in your Cisco Meraki Systems Manager.

Configure Cisco Meraki Systems Manager as an MDM/UEM Server

The images in this section display the Cisco Meraki Systems Manager GUI fields that you must work with during this task. The numbers in the images correspond to the step numbers in the task.

Figure 1: Steps To Configure Cisco Merki Systems Manager



Profile Configuration

Type: Device profile

Name: CiscoISEMDM

The name that will be shown to users

Description:

Optional

Profile Removal Policy

Removal Policy: Allow users to remove this profile

Targets

Group type: Manual | Named — Configure tags

Scope: All devices — Convert to target group

Installation target: All devices

Before you begin

In Cisco ISE, create and export a System Certificate that is configured for Admin usage. You will use this certificate in Step 12 of the following task.

For instructions on how to create and export a system certificate, see the topic "System Certificates" in Chapter "Basic Setup" in the *Cisco ISE Administrator Guide* for your release.

Step 1 Log in to your Cisco Meraki Systems Manager portal.

Step 2 From the main menu, go to **Systems Manager** > **Manage** > **Settings**.

Step 3 Click **+ Add Profile**.

Step 4 In the Add New Profile dialog box that is displayed, click the **Device profile (Default)** radio button.

Step 5 Click **Continue**.

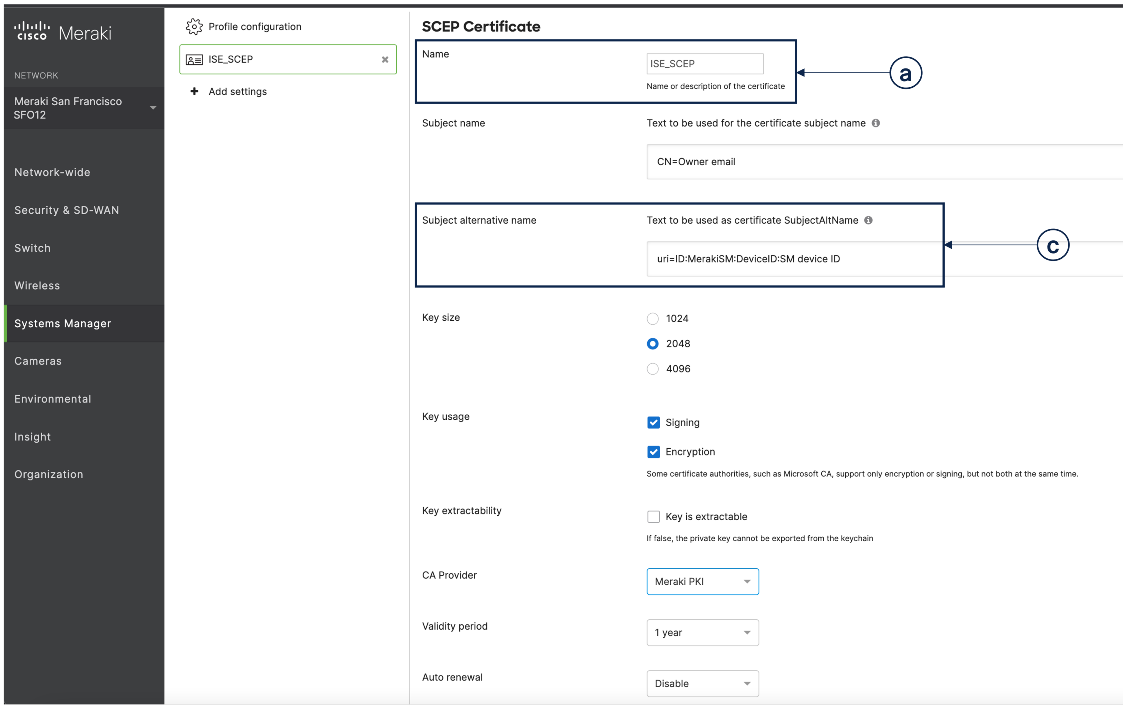
Step 6 In the **Name** and **Description** fields, enter the required values.

Step 7 Click **+Add settings**.

Step 8 In the **Add New Settings Payload** window that is displayed, click **SCEP Certificate.**

Step 9 In the **SCEP Certificate** window that is displayed:

Figure 2: The SCEP Certificate Configuration Window in Cisco Meraki Systems Manager



SCEP Certificate

Name: ISE_SCEP
Name or description of the certificate

Subject name: Text to be used for the certificate subject name
CN=Owner email

Subject alternative name: Text to be used as certificate SubjectAltName
uri=ID:MerakiSM:DeviceID:SM device ID

Key size: ○ 1024 ● 2048 ○ 4096

Key usage: ☑ Signing ☑ Encryption
Some certificate authorities, such as Microsoft CA, support only encryption or signing, but not both at the same time.

Key extractability: □ Key is extractable
If false, the private key cannot be exported from the keychain

CA Provider: Meraki PKI

Validity period: 1 year

Auto renewal: Disable

a) In the **Name** field, enter a name for the SCEP certificate. For example, **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 **$**, a drop-down list of variables is displayed. 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 CA provider from the drop-down list.
g) Click **Save**.

Step 10 Click **+Add settings**.

Step 11 In the **Add New Settings Payload** window that is displayed, click **Certificate**

Step 12 In the **Certificate** window that is displayed:

a) In the **Name** field, enter a name for the certifiate.
b) From the **CertStore** drop-down list, choose **System**.
c) In the **Certificate** field, click **Choose File** and upload the Cisco ISE system certificate that you downloaded as a prerequisite step for this task.
d) Click **Save**.

Step 13 Click **+Add settings**.

Step 14 In the **Add New Settings Payload** window that is displayed, click **WiFi Settings**.

Step 15 In the **WiFi Settings** window that is displayed:

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.

c) In the **Enterprise Settings** area that is displayed when you choose an enterprise option from the Security drop-down list:

1. In the **Protocol** tab, check the check box of any certificate-based protocol, such as TLS.
2. 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 Step 10).
3. In the **Trust** tab, in the **Trusted Certificates** area, check the check box next to the Cisco ISE certificate that you uploaded in Step 12.
4. Click **Save**.

Step 16 In the **Profile Configuration** tab, in the **Targets** area, add a tag for the ISE use case. For information on how to create and manage tags in Meraki Systems Manager, see Manage Tags. The application of tags ensures that the ISE profile with its certificate and Wi-Fi settings is applied to the relevant devices.

Step 17 In the **You have unsaved changes** dialog box, click **Save**.

Step 18 From the left menu pane, choose **Organization** > **Configure**> **MDM**

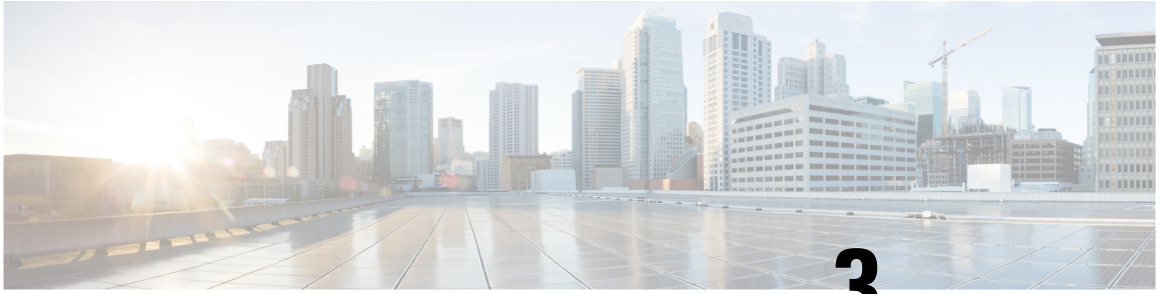
Step 19 From the ISE Settings area:

a) Take note of the username and password details that must be input in Cisco ISE.

b) To download the SCEP certificate that you must use in Cisco ISE, click the **Download** button.

What to do next

Now, connect Cisco Meraki Systems manager as an MDM server in Cisco ISE. For information on how to carry out this task, see "Configure Mobile Device Management Servers in Cisco ISE" in the Chapter "Secure Access" in the *Cisco ISE Administrator Guide* for your release.



CHAPTER 3

Integrate Microsoft Endpoint Manager Intune

- Introduction to Integrating Microsoft Intune with Cisco ISE, on page 9
- Configure Microsoft Endpoint Manager Intune, on page 10
- Manage VPN-Connected Mobile Devices with Microsoft Intune , on page 10
- Connect Microsoft Intune to Cisco ISE as a Mobile Device Management Server, on page 11

Introduction to Integrating Microsoft Intune with Cisco ISE

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

From March 24, 2024, Microsoft will no longer support the Intune NAC service API which supports MAC address and UDID-based queries. Only Microsoft Compliance Retrieval API, or NAC 2.0 API, will be supported. NAC 2.0 API supports GUID and MAC address-based queries since July 31, 2023.

After March 24, 2024, you must upgrade to one of the following 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, and Cisco ISE Release 3.0 and earlier, 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 the following endpoint attribute information:

- Compliance Status
- Managed by Intune
- MAC Address
- Registered Status

Configure Microsoft Endpoint Manager Intune

The following steps list the configurations that you usually carry out in Microsoft Endpoint Manager Intune. Choose the steps that you must implement according to your organization's needs. If you use Cisco ISE Release 3.1 and later releases, 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 as specified in Step 2 and Step 3. The SAN configuration allows Cisco ISE to receive a unique GUID for an endpoint from the Intune server to handle the issues that are presented by random and changing MAC addresses.

If you do not use the standard commercial Microsoft Azure environment, see the Microsoft National Cloud Deployments document for a list of Graph API endpoints that correspond to the various national clouds operated by Microsoft.

Step 1 Configure certificates for endpoint authentication in Microsoft Intune.

Step 2 Configure one of the following certificate management protocols and the corresponding certificate profiles, according to your organizational needs:

- Simple Certificate Enrollment Protocol (SCEP)

a. Configure infrastructure to support SCEP with Microsoft Intune.

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

- Private and public key infrastructure (PKI)

a. Configure and use PKCS certificates with Microsoft Intune.

b. Create a PKCS certificate profile.

Note When you configure an SCEP or a PKI profile, in the **Subject Alternative Name** area, choose **URI** as the **Attribute**, and **ID:Microsoft Endpoint Manager:GUID:{{DeviceId}}** as the **Value**.

Step 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, see 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

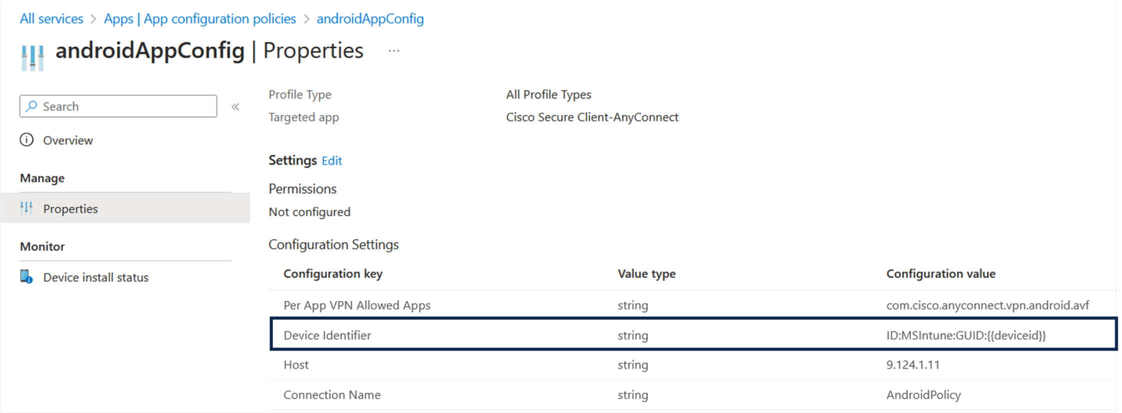
To manage VPN-connected mobile devices, the following configurations are required in Microsoft Intune.

- **Configure 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 connecting through the Cisco Secure Client-AnyConnect app. This policy must include the Device Identifier configuration key in its Configuration Settings.

Figure 3: App Configuration Policy Settings in Microsoft Intune



All services > Apps | App configuration policies > androidAppConfig

androidAppConfig | Properties ...

Profile Type	All Profile Types
Targeted app	Cisco Secure Client-AnyConnect

Settings Edit

Permissions

Not configured

Configuration Settings

Configuration key	Value type	Configuration value
Per App VPN Allowed Apps	string	com.cisco.anyconnect.vpn.android.avf
Device Identifier	string	ID:MSIntune:GUID:{{deviceid}}
Host	string	9.124.1.11
Connection Name	string	AndroidPolicy

- **Configure VPN-Connected iOS Device Settings in Microsoft Intune**

  For VPN-connected iOS devices, the VPN settings required in Microsoft Intune are detailed in Add VPN Settings on iOS and iPadOS devices in Microsoft Intune.

  Note that 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 the configurations are carried out, Cisco AnyConnect logs record the device identifier in the format **ID:Intune:DeviceID:<*device id*>**. Cisco ISE APIs retrieve this device ID for the endpoint and prioritize the device ID over the endpoint's MAC address when retrieving compliance information for the endpoint.

Connect Microsoft Intune to Cisco ISE as a Mobile Device Management 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.

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

- Cisco ISE Release 2.7 Patch 7 and later
- Cisco ISE Release 3.0 Patch 5 and later
- Cisco ISE Release 3.1 Patch 3 and later
- Cisco ISE Release 3.2 and later releases

For more information on the migration from Azure AD Graph to Microsoft Graph, see the following 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** field (Step 32).

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

Step 1 Log in to the Microsoft Azure portal, and navigate to **Azure Active Directory**.

Step 2 Choose **Manage** > **App registrations**.

Step 3 Click **New registration**.

Step 4 In the **Register an application** window that is displayed, enter a value in the **Name** field.

Step 5 In the **Supported Account Types** area, click the **Accounts in this organizational directory only** radio button.

Step 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.

Step 7 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **System** > **Certificates**.

Step 8 From the list of certificates displayed, check either the **Default self-signed server certificate** check box or the check box that is adjacent to or any other certificate that you have configured for **Admin** usage.

Step 9 Click **Export**.

Step 10 In the dialog box that is displayed, click the **Export Certificate Only** radio button and click **Export**.

Step 11 Click **View** to see the details of this certificate. Scroll down the displayed **Certificate Hierarchy** dialog box to the **Fingerprints** area. (You have to refer to these values at a later step.)

Step 12 In the Microsoft Azure Active Directory portal, click **Certificates & secrets** in the left pane.

Step 13 Click **Upload certificate** and upload the certificate that you exported from Cisco ISE.

Step 14 After the certificate is uploaded, verify that the **Thumbprint** value that is displayed in the window matches the **Fingerprint** value in the Cisco ISE certificate (Step 11).

Step 15 Click **Manifest** in the left pane.

Step 16 In the content displayed, check the value of **displayName**. The value must match the common name that is mentioned in the Cisco ISE certificate.

Step 17 Click **API permissions** in the left pane.

Step 18 Click **Add a permission** and add the following permissions:

API / Permission Name	Type	Description
Intune		
get_device_compliance	Application	Get device state and compliance information from Microsoft Intune.
Microsoft Graph		
Directory.Read.All	Delegated	Read the directory data.
Directory.Read.All	Application	Read the directory data.

API / Permission Name	Type	Description
offline_access	Delegated	Maintain access to data you have given it access to.
openid	Delegated	Sign in the users.
User.Read	Delegated	Sign in the users and read the user profiles.
User.Read.All	Delegated	Read the full profiles of all the users.
User.Read.All	Application	Read the full profiles of all the users.

Step 19 From the left pane, choose **API permissions** > **Add a permission** > **APIs my organization uses**.

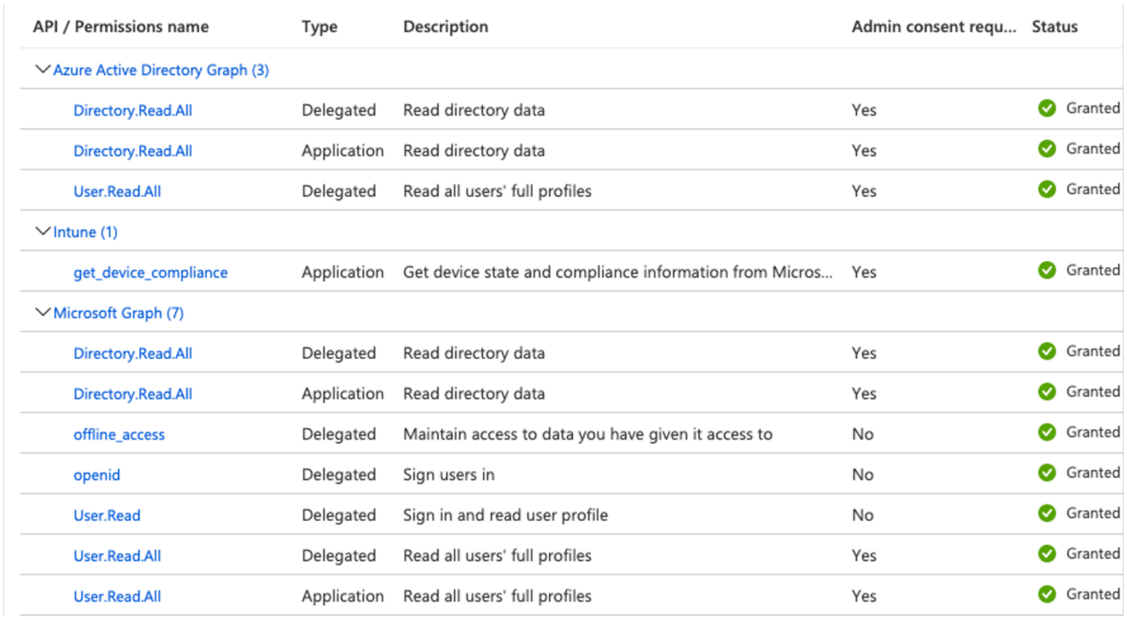
Step 20 Search for **Windows Azure Active Directory**, and choose the same from the search results.

Step 21 Add the following permissions:

API / Permissions Name	Type	Description
Azure Active Directory Graph		
Directory.Read.All	Delegated	Read the directory data
Directory.Read.All	Application	Read the directory data
User.Read.All	Delegated	Read the full profiles of all the users

The final table after adding the permissions must look like the following:

Figure 4: The APIs and Permissions That Must Be Configured in Microsoft Intune



API / Permissions name	Type	Description	Admin consent requ...	Status
Azure Active Directory Graph (3)				
Directory.Read.All	Delegated	Read directory data	Yes	✓ Granted
Directory.Read.All	Application	Read directory data	Yes	✓ Granted
User.Read.All	Delegated	Read all users' full profiles	Yes	✓ Granted
Intune (1)				
get_device_compliance	Application	Get device state and compliance information from Micros...	Yes	✓ Granted
Microsoft Graph (7)				
Directory.Read.All	Delegated	Read directory data	Yes	✓ Granted
Directory.Read.All	Application	Read directory data	Yes	✓ Granted
offline_access	Delegated	Maintain access to data you have given it access to	No	✓ Granted
openid	Delegated	Sign users in	No	✓ Granted
User.Read	Delegated	Sign in and read user profile	No	✓ Granted
User.Read.All	Delegated	Read all users' full profiles	Yes	✓ Granted
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted

Step 22 Click **Grant admin consent for <*tenant name*>**.

Step 23 Make a note of the following details from the **Overview** window of the application:

- **Application (client) ID**
- **Directory (tenant) ID**

Step 24 Click **Endpoints** in the **Overview** window and make a note of the value in the **Oauth 2.0 token endpoint (V2)** field.

Step 25 Download the following certificates from https://www.digicert.com/kb/digicert-root-certificates.htm in the PEM (chain) format:

- Baltimore CyberTrust Root
- DigiCert SHA2 Secure Server CA
- DigiCert Global Root CA
- DigiCert Global Root G2
- Microsoft Azure TLS Issuing CA 01
- Microsoft Azure TLS Issuing CA 02
- Microsoft Azure TLS Issuing CA 05
- Microsoft Azure TLS Issuing CA 06

You can download Microsoft Azure TLS Issuing CA certificates from the Microsoft PKI repository. Cisco ISE requires trusted communication to Microsoft Intune using the preceding certificates. Make sure to download the certificates required for trusted communication between Cisco ISE and Microsoft Intune. Microsoft releases new certificates periodically; newer certificates might be available.

Note Microsoft Intune certificates have been updated. You may need to import new root certificates to enable a successful connection between Microsoft Intune and Cisco ISE. See Intune certificate updates: Action may be required for continued connectivity.

Step 26 In the Cisco ISE administration portal, click the **Menu** icon (☰) and choose **Administration** > **System** > **Certificates** > **Trusted Certificates**.

Step 27 For each of the four certificates that you have downloaded, carry out the following steps:

a. Click **Import**.

b. Click **Choose File** and choose the corresponding downloaded certificate from your system.

c. Allow the certificate to be trusted for use by Infrastructure and Cisco Services. In the **Usage** area, check the **Trust for authentication within ISE** and **Trust for authentication of Cisco Services** check boxes.

d. Click **Save**.

Step 28 Click the **Menu** icon (☰) and choose **Administration** > **Network Resources** > **External MDM**.

Step 29 Click **Add**.

Step 30 Enter a value in the **Name** field.

Step 31 From the **Authentication Type** drop-down list, choose **OAuth – Client Credentials**.

Step 32 The following fields require the information from the Microsoft Intune application in the Microsoft Azure Active Directory:

- In the **Auto Discovery URL** field, enter **https://graph.microsoft.com**.

Note 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 June 30, 2023. Upgrade to a Cisco ISE release that supports Microsoft Graph for successful integration.

The following are the Cisco ISE releases that support Microsoft Graph applications:

- Cisco ISE Release 2.7 Patch 7 and later
- Cisco ISE Release 3.0 Patch 5 and later
- Cisco ISE Release 3.1 Patch 3 and later
- Cisco ISE Release 3.2 and later releases

- In the **Client ID** field, enter the **Application (client) ID** value from the Microsoft Intune application.
- In the **Token Issuing URL** field, enter the **Oauth 2.0 Token Endpoint (V2)** value.
- In the **Token Audience** field, enter **https://api.manage.microsoft.com//.default** if you use the following releases of Cisco ISE:
  - Cisco ISE Release 3.0 Patch 8 and later releases
  - Cisco ISE Release 3.1 Patch 8 and later releases
  - Cisco ISE Release 3.2 Patch 3 and later releases
  - Cisco ISE Release 3.3 and later releases

Note 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** in Step 31. 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, see Migrate applications to the Microsoft Authentication Library (MSAL).

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

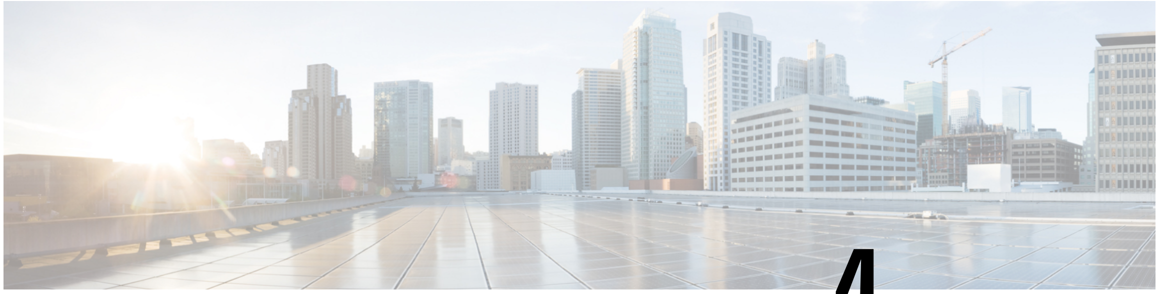
Step 33 Enter the required values for the **Polling Interval** and **Time Interval For Compliance Device ReAuth Query** fields.

Step 34 Click **Test Connection** to ensure that Cisco ISE can connect to the Microsoft server.

Step 35 When the connection test is successful, choose **Enabled** from the **Status** drop-down list.

Step 36 Click **Save**.

Step 37 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.



CHAPTER 4

Integrate Ivanti (previously MobileIron) UEM

- Configure Ivanti (Previously MobileIron) Unified Endpoint Management Servers, on page 17

Configure Ivanti (Previously MobileIron) Unified Endpoint Management Servers

Note MobileIron has been acquired by Ivanti. MobileIron continues to offer Unified Endpoint Management (UEM) solutions such as MobileIron Core (On-Premise) and MobileIron Cloud at the time of writing this document.

Cisco ISE Release 3.1 leverages APIs through the BasicAuth framework to connect to MobileIron Core or MobileIron Cloud servers and receive GUID values from these servers. Cisco ISE then uses the GUID values instead of MAC addresses to identify endpoints, enabling reliable authentication even when MAC Address Randomization is in use.

GUID-based authentication occurs through the use of client certificates, also known as X509 or Identity Certificates. Perform the following tasks to configure the certificates sent from MobileIron Cloud or MobileIron Core servers to Cisco ISE to include GUID values.

MobileIron Core 11.3.0.0 Build 24 and later releases support the provision of GUID to Cisco ISE.

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.
3. Configure an Identity Certificate to include GUID information.
4. Upload root or trusted certificates, as required.
5. Configure a Wi-Fi profile.

Note 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 the connected managed devices. MobileIron does not recommend the use of self-signed certificates or local CA. This guide details the steps for self-signed certificates and a local CA only as an example, to highlight the Subject and Subject Alternative Name attribute configurations that are necessary for handling random and changing MAC addresses in Cisco ISE Release 3.1.

In Cisco ISE:

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

Configure MobileIron Cloud UEM Servers

The following sections comprise the various procedures that are a part of the larger MobileIron Cloud UEM server configuration.

Create a MobileIron Cloud User Account and Assign the Cisco ISE Operations Role

Step 1 Log in to the MobileIron Cloud portal.

Step 2 From the top menu, choose **Users**.

Step 3 From the **Add** drop-down list, choose **Add API User**.

Step 4 In the **Add API User** window, enter values for the following fields:

- **Username**
- **Email Address**
- **First Name**
- **Last Name**
- **Password**
- **Confirm Password**

Step 5 To allow a user to invoke the APIs required for Cisco ISE integration, in the **Assign Roles** area, check the **Cisco ISE Operations** check box.

Step 6 Click **Done**.

Configure a Certificate Authority in MobileIron Cloud

This procedure describes how to configure a local CA. However, MobileIron Cloud allows you to choose from a wider range of CA configurations. Choose the option that best suits your organization’s requirements.

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

Step 1 In the MobileIron Cloud portal, choose **Admin** > **Certificate Management**.

Step 2 Click **Add**.

Step 3 Click **Create a Standalone Certificate Authority**.

Step 4 In the dialog box that is displayed, enter the details in the following fields:

a. **Name**

b. In the **Subject Parameters** area, enter a value for at least one of the following fields:

- **Common Name**
- **Email**
- **Organisation Unit**
- **Organisation**
- **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 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 so that it is distributed to the connected devices. This allows the devices to trust the source or the issuer of the identity certificate that is used for authentication.

Step 1 From the MobileIron Cloud menu, choose **Configurations**.

Step 2 Click **Add** and choose **Certificate**.

Step 3 In the **Name** field, enter a name for the trusted certificate.

Step 4 In the **Configuration Setup** area, click **Choose File** and choose the trusted or root certificate for your CA.

Step 5 Click **Next**.

Configure an Identity Certificate in MobileIron Cloud

Configure an Identity Certificate in MobileIron Cloud to define 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 Certificate Authority as the source.

Note If you have existing Identity Certificates in MobileIron Cloud that are configured for Cisco ISE MDM use cases, modify the certificate according to Step 5 of this procedure to receive GUID information from MobileIron servers.

Step 1 From the MobileIron Cloud top menu, choose **Configurations** and click **Identity Certificate**.

Step 2 In the **Name** field, enter a value.

Step 3 In the **Configuration Setup** area, from the drop-down list, choose **Dynamically Generated**.

Step 4 From the **Source** drop-down list, choose the CA that you configured in the procedure Configure a Certificate Authority in MobileIron Cloud.

Step 5 From the **Subject Alternative Name Type** drop-down list, choose **Uniform Resource Identifier**.

Step 6 In the **Subject Alternative Name Value** field, enter **ID:Mobileiron:GUID:${deviceGUID}**. We recommend that you configure the Subject Alternative Name field for GUID.

Step 7 (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}**.

Step 8 Click **Test Configuration and Continue**.
The **Configuration Test Successful** dialog box displays the details of the identity certificate created.

Step 9 In the **Distribute** window, click **Custom**.

Step 10 In the **Define Device Group Distribution** area, check the check boxes for the device groups that you want to distribute in this configuration.

Step 11 Click **Done**.

Step 12 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.

Configure a Wi-Fi 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 GUID in the Subject or Subject Alternative Name attributes.

Step 1 From the MobileIron Cloud menu, choose **Configurations** and click **Wi-Fi**.

Step 2 In the **Name** field, enter a value.

Step 3 In the **Service Set Identifier (SSID)** field, enter the name of your network.

Step 4 The **Auto Join** check box is checked by default. Do not make any changes.

Step 5 From the **Security Type** drop-down list, choose the required option.

Step 6 In the **Enterprise Settings** area, in the **Protocols** tab, check the **TLS** check box.

Step 7 In the **Authentication** tab, enter the required values in the **Username** and **Password** fields.

Step 8 From the **Identity Certificate** drop-down list, choose the identity certificate that you created in the procedure Configure an Identity Certificate in MobileIron Cloud, on page 20.

Step 9 (Optional) In the **Trust** tab, check the check box adjacent to the trusted certificate that you want to use.

Step 10 In the **All Versions** area, from the **Network Type** drop-down list, choose **Standard**.

Step 11 Click **Next**.

Step 12 In the **Distribute** window, click the required option.

Step 13 In the **Define Device Group Distribution** area, check the check boxes adjacent to the device groups that you want to include in this configuration.

Step 14 Click **Done**.

Configure MobileIron Core UEM Servers

The following sections comprise the various procedures that are a part of the larger MobileIron Core UEM server configuration.

Create a MobileIron Core User and Assign API Permissions

Step 1 Log in to your MobileIron Core administrator portal.

Step 2 Choose **Devices and Users** > **Users**.

Step 3 From the **Add** drop-down list, choose **Add Local User**.

Step 4 Enter the required values in the following fields:

- **User ID**
- **First Name**
- **Last Name**
- **Password**
- **Confirm Password**
- **Email**

Step 5 Click **Save**.

Step 6 To assign an API role to the newly created user, click **Admin** and check the check box next to the corresponding user name.

Step 7 From the **Actions** drop-down list, choose **Assign to Space**.

Step 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 options displayed. The user that you have created must have tenant administrator persmissions, and the **API role** must be enabled for this user.

Step 9 Click **Save**.

Configure a Certificate Authority in MobileIron Core

MobileIron Core allows you to choose from a wider range of CA configurations. Choose the option that best suits your organization's requirements. This procedure details the steps for self-signed certificates only as an example.

Step 1 In the MobileIron Core administrator portal, choose **Services** > **Local CA**.

Step 2 From the **Add** drop-down list, choose **Generate Self-Signed Cert**.

Step 3 In the **Generate Self-Signed Certificate** dialog box that is displayed, enter the required values in the following fields:

- **Local CA Name**
- **Key Length**
- **CSR Signature Algorithm**
- **Key Lifetime (in days)**
- **Issuer Name**

Step 4 Click **Generate**.

Step 5 Download the CA certificate because you must upload this certificate in Cisco ISE at a later stage. Click **View Certificate** next to the certificate that you want to download, and copy all the contents into the dialog box that is displayed. Paste this content in a text editor of your choice and save the document as a .cer file.

Upload Root or Trusted Certificates in MobileIron Core

Step 1 In the MobileIron Core administrator portal, choose **Policies and Configs** > **Configurations**.

Step 2 From the **Add New** drop-down list, choose **Certificates**.

Step 3 In the **New Certificate Setting** dialog box that is displayed, enter a name and description for the certificate in the corresponding fields.

Step 4 In the **File Name** area, click **Browse** and choose the root or trusted certificate you need to upload for the CA that you configured earlier.

The accepted file types are .cer, .crt, .pem, and .der.

Step 5 Click **Save**.

Configure Certificate Enrollment in MobileIron Core

This procedure details the steps to connect a local CA only as an example, to highlight the Subject and Suject Alternative Name attribute configurations that are necessary for handling random and changing MAC addresses in Cisco ISE Release 3.1. MobileIron does not recommend the use of self-signed certificates or local CA.

Step 1 In the MobileIron Core administrator portal, choose **Policies and Configs** > **Configurations**.

Step 2 Click **Add New**, choose **Certificate Enrollment** and then choose the appropriate connector for the CA you have configured. Choose **Local** if you are configuring a local CA.

This procedure describes the steps for a local CA. You must choose the certificate enrollment option according to the CA that you have configured for the purpose of connecting your MobileIron Core servers to Cisco ISE.

Step 3 In the **New Local Certificate Enrollment Setting** dialog box that is displayed, provide values for the following 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 3.1 and later releases, 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}** to use this field to share the UUID (referred to as GUID in Cisco ISE) with Cisco ISE 3.1 and later releases.

Step 4 Click **Issue Test Certificate**.

Configure a Wi-Fi Profile in MobileIron Core

Step 1 In the MobileIron Core administrator portal, choose **Policies and Configs** > **Configurations**.

Step 2 From the **Add New** drop-down list, choose **Wi-Fi**.

Step 3 In the **New Wi-Fi Setting** dialog box, enter the required values in the following 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 Configure Certificate Enrollment in MobileIron Core, on page 22.
- Click **Save**.

Map Resources to Labels in MobileIron Core

Configure a label to define the configurations, rules, and profiles that must be applied to a group of endpoints and devices. You can use a label to group endpoints and devices based on a wide range of criteria, including organizational unit, device types, operating systems that are running in an endpoint, and so on. After you create a label, assign this label to various resources in the **Policies & Configs** windows to map the configurations, policies, and device or user groups to each other.

To map and distribute the configurations and policies for the Cisco ISE use case, configure an appropriate label, and apply the Certificate Enrollment, Wi-Fi profile, and any other configuration you create for this use case, to the label.

Step 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**.

Step 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**.

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.