Integrate Microsoft Endpoint Manager Intune

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

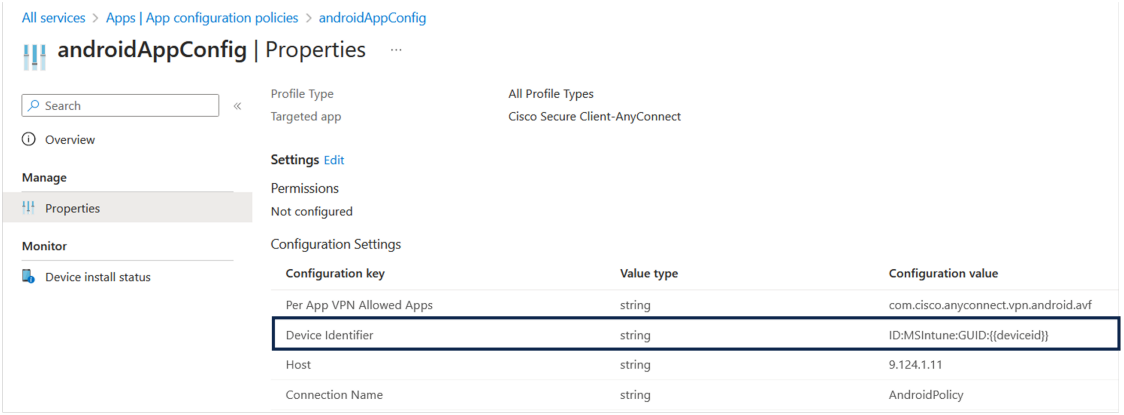
To manage VPN-connected mobile devices, the following configurations are required in Microsoft Intune.

- **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 1: App Configuration Policy Settings in Microsoft Intune



- **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 2: 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.