Integrate Ivanti (previously MobileIron) UEM

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 4.

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 6.
- 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**.