Cisco Cloud APIC Security

This chapter contains the following sections:

Access, Authentication, and Accounting

Cisco Cloud Application Policy Infrastructure Controller (Cloud APIC) policies manage the authentication, authorization, and accounting (AAA) functions. The combination of user privileges, roles, and domains with access rights inheritance enables administrators to configure AAA functions at the managed object level in a granular fashion. These configurations can be implemented using the REST API or the GUI.

Note There is a known limitation where you cannot have more than 32 characters for the login domain name. In addition, the combined number of characters for the login domain name and the user name cannot exceed 64 characters.

For more access, authentication, and accounting configuration information, see *Cisco APIC Security Configuration Guide, Release 4.0(1)* at https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html.

Configuration

The admin account is configured in the initial configuration script, and the admin is the only user when the system starts.

Configuring a Local User

Refer to Creating a Local User Using the Cisco Cloud APIC GUI to configure a Local User and associate it to the OTP, SSH Public Key, and X.509 User Certificate using the Cloud APIC GUI.

Configuring TACACS+, RADIUS, LDAP and SAML Access

The following topics describe how to configure TACACS+, RADIUS, LDAP and SAML access for the Cloud APIC.

Overview

This topic provides step-by-step instructions on how to enable access to the Cloud APIC for RADIUS, TACACS+, LDAP, and SAML users, including ADFS, Okta, and PingID.

For additional TACACS+, RADIUS, LDAP, and SAML information, see *Cisco APIC Security Configuration Guide, Release 4.0(1)* at https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html.

Configuring Cloud APIC for TACACS+ Access

Before you begin

- The Cloud Application Policy Infrastructure Controller (Cloud APIC) is online.

- The TACACS+ server host name or IP address, port, and key are available.

- The Cloud APIC management endpoint group is available.

Step 1 In the Cloud APIC, create the **TACACS+ Provider**.

a) On the menu bar, choose **Administrative** > **Authentication**.

b) In the Work pane, click on **Providers** tab and then click on the **Actions** drop-down and select **Create Provider**.

The **Create Provider** dialog box appears.

c) In the **Host Name/IP Address** field, enter the Host Name/IP Address of the provider.

d) In the **Description** field, enter a description of the provider.

e) Click the **Type** drop-down list and choose **TACACS+**.

f) In **Settings** section, specify the **Key**, **Port**, **Authentication Protocol**, **Timeout**, **Retries**, **Management EPG**. Select either **Enabled** or **Disabled** for **Server Monitoring**.

Step 2 Create the **Login Domain** for TACACS+.

a) Click the **Intent** icon.

The **Intent** menu appears.

b) Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

A list of **Administrative** options appear in the **Intent** menu.

c) From the **Administrative** list in the **Intent** menu, click **Create Login Domain**.

The **Create Login Domain** dialog box appears.

d) Enter the appropriate values in each field as listed in the following *Create Login Domain Dialog Box Fields* table then continue.

Properties	Description
General	
Name	Enter the name of the Login Domain
Description	Enter the description of the Login Domain.
Settings	
Realm	Choose **TACACS+** from the dropdown menu
Providers	To choose a Provider(s): 1. Click **Add Providers**. The **Select Providers** dialog appears. 2. Click to choose a provider(s) in the column on the left. 3. Click **Select**. You return to the **Create Login Domain** dialog box.

e) Click **Save** to save the configuration.

What to do next

This completes the APIC TACACS+ configuration steps. Next, if a RADIUS server will also be used, configure the APIC for RADIUS.

Configuring Cloud APIC for RADIUS Access

Before you begin

- The Cloud Application Policy Infrastructure Controller (Cloud APIC) is online.

- The RADIUS server host name or IP address, port, and key are available.

- The Cloud APIC management endpoint group is available.

Step 1 In the Cloud APIC, create the **RADIUS Provider**.

a) On the menu bar, choose **Administrative** > **Authentication**.

b) In the Work pane, click on **Providers** tab and then click on the **Actions** drop-down and select **Create Provider**.

The **Create Provider** dialog box appears.

c) In the **Host Name/IP Address** field, enter the Host Name/IP Address of the provider.

d) In the **Description** field, enter a description of the provider.

e) Click the **Type** drop-down list and choose **RADIUS**.

f) In the **Settings** section, specify the **Key**, **Port**, **Authentication Protocol**, **Timeout**, **Retries**, **Management EPG**. Select either **Enabled** or **Disabled** for **Server Monitoring**.

Step 2 Create the **Login Domain** for **RADIUS**.

a) Click the **Intent** icon.

The **Intent** menu appears.

b) Click the drop-down arrow below the **Intent** search box and choose **Administrative**

A list of **Administrative** options appear in the **Intent** menu.

c) From the **Administrative** list in the **Intent** menu, click **Create Login Domain**.

The **Create Login Domain** dialog box appears.

d) Enter the appropriate values in each field as listed in the following *Create Login Domain Dialog Box Fields* table then continue.

Properties	Description
General	
Name	Enter the name of the Login Domain
Description	Enter the description of the Login Domain.
Settings	
Realm	Choose **RADIUS** from the dropdown menu
Providers	To choose a Provider(s): 1. Click **Add Providers**. The **Select Providers** dialog appears. 2. Click to choose a provider(s) in the column on the left. 3. Click **Select**. You return to the **Create Login Domain** dialog box.

e) Click **Save** to save the configuration.

What to do next

This completes the Cloud APIC RADIUS configuration steps. Next, configure the RADIUS server.

Configuring a Cisco Secure Access Control Server for RADIUS and TACACS+ Access to the Cloud APIC

Refer to the section *Configuring a Cisco Secure Access Control Server for RADIUS and TACACS+ Access to the APIC* in the **Cisco APIC Security Configuration Guide, Release 4.0(1)** at
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html.

Configuring LDAP Access

There are two options for LDAP configurations:

- Configure a Cisco AVPair

- Configure LDAP group maps in the cloud APIC

The following sections contain instructions for both configuration options.

Configuring Windows Server 2008 LDAP for APIC Access with Cisco AVPair

Refer to the section *Configuring Windows Server 2008 LDAP for APIC Access with Cisco AVPair* in the **Cisco APIC Security Configuration Guide, Release 4.0(1)** at
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html.

Configuring Cloud APIC for LDAP Access

Before you begin

- The Cloud Application Policy Infrastructure Controller (Cloud APIC) is online.

- The LDAP server host name or IP address, port, bind DN, Base DN, and password are available.

- The cloud APIC management endpoint group is available.

Step 1 In the Cloud APIC, create the **LDAP Provider**.

    a) On the menu bar, choose **Administrative** > **Authentication**.

    b) In the Work pane, click on **Providers** tab and then click on the **Actions** drop-down and select **Create Provider**.

       The **Create Provider** dialog box appears.

    c) In the **Host Name/IP Address** field, enter the Host Name/IP Address of the provider.

    d) In the **Description** field, enter a description of the provider.

    e) Click the **Type** drop-down list and choose **LDAP**.

    f) Specify the **Bind DN**, **Base DN**, **Password**, **Port**, **Attribute**, **Filter Type** and **Management EPG**.

Note	• The bind DN is the string that the Cloud APIC uses to log in to the LDAP server. The Cloud APIC uses this account to validate the remote user attempting to log in. The base DN is the container name and path in the LDAP server where the Cloud APIC searches for the remote user account. This is where the password is validated. Filter is used to locate the attribute that the Cloud APIC requests to use for the *cisco-av-pair*. This contains the user authorization and assigned RBAC roles for use on the Cloud APIC. The Cloud APIC requests the attribute from the LDAP server.

- **Attribute** field—Enter one of the following:
    - For LDAP server configurations with a Cisco AVPair, enter **CiscoAVPair**.
    - For LDAP server configurations with an LDAP group map, enter **memberOf**.

Step 2   Create the **Login Domain** for LDAP.

    a) On the menu bar, choose **Administrative** > **Authentication**.

    b) In the Work pane, click on **Login Domains** tab and then click on the **Actions** drop-down and select **Create Login Domain**.

    c) Enter the appropriate values in each field as listed in the following *Create Login Domain Dialog Box Fields* table then continue.

Properties	Description
General	
Name	Enter the name of the Login Domain
Description	Enter the description of the Login Domain.
Settings	
Realm	Choose **LDAP** from the dropdown menu
Providers	To choose a Provider(s): 1. Click **Add Providers**. The **Select Providers** dialog appears. 2. Click to choose a provider(s) in the column on the left. 3. Click **Select**. You return to the **Create Login Domain** dialog box.

Properties	Description

Authentication Type	1. Select **Cisco AV Pairs**, if provider(s) was configured with **CiscoAVPair** as the **Attribute**.
	
	2. Select **LDAP Group Map Rules**, if provider(s) was configured with **memberOf** as the **Attribute**.
	
	   a. Click **Add LDAP Group Map Rule**. The dialog box appears.
	
	   b. Specify the map rule **Name**, **Description** (optional), and **Group DN**.
	
	   c. Click the + next to **Add Security Domain**. The dialog box appears.
	
	   d. Click the + to access the **Role** name and Role **Privilege** Type (**Read** or **Write**) fields. Click check mark.
	
	   e. Repeat step 4 to add more roles. Then click **Add**.
	
	   f. Repeat step 3 to add more security domains. Then click **Add**.

d) Click **Save** on Create Login Domain dialog box.

Configuring Cloud APIC for SAML Access

The following sections provide detailed information on configuring Cloud APIC for SAML access.

About SAML

Refer to the section *About SAML* in the **Cisco APIC Security Configuration Guide, Release 4.0(1)** at
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html.

Basic Elements of SAML

Refer to the section *Basic Elements of SAML* in the **Cisco APIC Security Configuration Guide, Release 4.0(1)** at
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html.

Supported IdPs and SAML Components

Refer to the section *Supported IdPs and SAML Components* in the **Cisco APIC Security Configuration Guide, Release 4.0(1)** at
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html.

Configuring Cloud APIC for SAML Access

> **Note** SAML based Authentication is only for Cloud APIC GUI and not for REST.

Before you begin

- The SAML server host name or IP address, and the IdP's metadata URL are available.

- The Cloud APIC management endpoint group is available.

- Set up the following:

  - Time Synchronization and NTP

  - Configuring a DNS Provider Using the GUI

  - Configuring a Custom Certificate for Cisco ACI HTTPS Access Using the GUI

Step 1 In the Cloud APIC, create the **SAML Provider**.

a) On the menu bar, choose **Administrative** > **Authentication**.
b) In the **Work** pane, click on **Providers** tab and then click on the **Actions** drop-down and select **Create Provider**.
c) In the **Host Name/IP Address** field, enter the Host Name/IP Address of the provider.
d) In the **Description** field, enter a description of the provider.
e) Click the **Type** drop-down list and choose **SAML**.
f) In **Settings** pane, perform following:

- Specify the IdP metadata URL:

  - In case of AD FS, IdP Metadata URL is of the format *https://<FQDN ofADFS>/FederationMetadata/2007-06/FederationMetadata.xml*.

  - In case of Okta, to get the IdP Metadata URL, copy the link for **Identity Provider Metadata** in the **Sign On** section of the corresponding SAML Application from the Okta server.

- Specify the **Entity ID** for the SAML-based service.

- Configure the **HTTPS Proxy for Metadata URL** if it is needed to access the IdP metadata URL.

- Select the **Certificate Authority** if IdP is signed by a Private CA.

- Select the **Signature Algorithm Authentication User Requests** from the drop-down.

- Select checkbox to enable **Sign SAML Authentication Requests**, **Sign SAML Response Message**, **Sign Assertions in SAML Response**, **Encrypt SAML Assertions**.

g) Click **Save** to save the configuration.

Step 2 Create the login domain for SAML.

a) On the menu bar, choose **Administrative** > **Authentication**.
b) In the **Work** pane, click on the **Login Domains** tab and then click on the **Actions** drop-down and select **Create Login Domain**.

c) Enter the appropriate values in each field as listed in the following Create Login Domain Dialog Box Fields table then continue.

Properties	Description
General	
Name	Enter the name of the Login Domain
Description	Enter the description of the Login Domain.
Settings	
Realm	Choose **SAML** from the dropdown menu
Providers	To choose a Provider(s): 1. Click **Add Providers**. The **Select Providers** dialog appears. 2. Click to choose a provider(s) in the column on the left. 3. Click **Select**. You return to the **Create Login Domain** dialog box.

d) Click **Save** to save the configuration.

Setting Up a SAML Application in Okta

Refer to the section *Setting Up a SAML Application in Okta* of ***Cisco APIC Security Configuration Guide, Release 4.0(1)*** at
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html.

Setting Up a Relying Party Trust in AD FS

Refer to the section *Setting Up a Relying Party Trust in AD FS* in the ***Cisco APIC Security Configuration Guide, Release 4.0(1)*** at
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html.

Configuring HTTPS Access

The following sections describe how to configure HTTPS access.

About HTTPS Access

This article provides an example of how to configure a custom certificate for HTTPS access when using Cisco ACI.

For more information, see the section *HTTPS Access* in the ***Cisco APIC Security Configuration Guide, Release 4.0(1)*** at https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html.

Guidelines for Configuring Custom Certificates

- Wild card certificates (such as *.cisco.com, which is used across multiple devices) and its associated private key generated elsewhere are not supported on the Cisco Cloud APIC as there is no support to input the private key or password in the Cisco Cloud APIC. Also, exporting private keys for any certificates, including wild card certificates, is not supported.

- You must download and install the public intermediate and root CA certificates before generating a Certificate Signing Request (CSR). Although a root CA Certificate is not technically required to generate a CSR, Cisco requires the root CA certificate before generating the CSR to prevent mismatches between the intended CA authority and the actual one used to sign the CSR. The Cisco Cloud APIC verifies that the certificate submitted is signed by the configured CA.

- To use the same public and private keys for a renewed certificate generation, you must satisfy the following guidelines:

    - You must preserve the originating CSR as it contains the public key that pairs with the private key in the key ring.

    - The same CSR used for the originating certificate must be resubmitted for the renewed certificate if you want to re-use the public and private keys on the Cisco Cloud APIC.

    - Do not delete the original key ring when using the same public and private keys for the renewed certificate. Deleting the key ring will automatically delete the associated private key used with CSRs.

- Only one Certificate Based Root can be active per pod.

- Client Certificate based authentication is not supported for this release.

Configuring a Custom Certificate for Cisco ACI HTTPS Access Using the GUI

Determine from which authority you will obtain the trusted certification so that you can create the appropriate Certificate Authority.

Before you begin

CAUTION: PERFORM THIS TASK ONLY DURING A MAINTENANCE WINDOW AS THERE IS A POTENTIAL FOR DOWNTIME. Expect a restart of all web servers on Cloud APIC during this operation.

Step 1 On the menu bar, choose **Administrative** > **Security**.

Step 2 In the Work pane, click on **Certificate Authorities** tab and then click on the **Actions** drop-down and select **Create Certificate Authority**.

Step 3 In the **Create Certificate Authority** dialog box, in the **Name** field, enter a name for the certificate authority and in the **Description** field, enter a description.

Step 4 Select **System** in the **Used for** field.

Step 5 In the **Certificate Chain** field, copy the intermediate and root certificates for the certificate authority that will sign the Certificate Signing Request (CSR) for the Cloud Application Policy Infrastructure Controller (APIC). The certificate should be in Base64 encoded X.509 (CER) format. The intermediate certificate is placed before the root CA certificate. It should look similar to the following example:

```
-----BEGIN CERTIFICATE-----
<Intermediate Certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA Certificate>
-----END CERTIFICATE-----
```

Step 6 Click **Save**.

Step 7 On the menu bar, choose **Administrative** > **Security**.

Step 8 In the Work pane, click on the **Key Rings** tab, then click on the Actions drop-down and select **Create Key Ring**.

Step 9 In the **Create Key Ring** dialog box, enter a name for the key ring in the **Name** field and a description in the **Description** field.

Step 10 Select **System** in the **Used for** field.

Step 11 For the **Certificate Authority** field, click on **Select Certificate Authority**and select the Certificate Authority that you created earlier.

Step 12 Select either **Generate New Key** or **Import Existing Key** for the field **Private Key**. If you select **Import Existing Key**, enter a private key in the **Private Key** text box.

Step 13 Select modulus from the **Modulus** drop-down. menu

Step 14 In the **Certificate** field, do not add any content.

Step 15 Click **Save**.

In the **Work** pane, in the **Key Rings** area, the **Admin State** for the key ring created displays **Started**.

Step 16 Double-click on the created Key Ring to open **Key Ring** *key_ring_name* dialog box from the **Work** pane.

Step 17 In the **Work** pane, click on **Create Certificate Request**.

Step 18 In the **Subject** field, enter the fully qualified domain name (FQDN) of the Cloud APIC.

Step 19 Fill in the remaining fields as appropriate.

Step 20 Click **Save**.

The **Key Ring** *key_ring_name* dialog box appears.

Step 21 Copy the contents from the field Request to submit to the **Certificate Authority** for signing.

Step 22 From the **Key Ring** *key_ring_name* dialog box, click on edit icon to display the **Key Ring** *key_ring_name* dialog box.

Step 23 In the **Certificate** field, paste the signed certificate that you received from the certificate authority.

Step 24 Click **Save** to return to the **Key Rings** work pane.

The key is verified, and in the **Work** pane, the **Admin State** changes to **Completed** and is now ready for use in the HTTPs policy.

Step 25 Navigate to **Infrastructure** > **System Configuration**, then click the **Management Access** tab.

Step 26   Click the edit icon on the **HTTPS** work pane to display the **HTTPS Settings** dialog box.

Step 27   Click on **Admin Key Ring** and associate the Key Ring that you created earlier.

Step 28   Click **Save**.

All web servers restart. The certificate is activated, and the non-default key ring is associated with HTTPS access.

What to do next

You must remain aware of the expiration date of the certificate and take action before it expires. To preserve the same key pair for the renewed certificate, you must preserve the CSR, as it contains the public key that pairs with the private key in the key ring. Before the certificate expires, the same CSR must be resubmitted. Do not delete or create a new key ring, as deleting the key ring will delete the private key stored internally on the Cloud APIC.