Authentication and SSO Configurations

Managing Cisco MSX Authentication 2

Retrieving the Device Password 13

Revised: May 20, 2022

Back

Managing Cisco MSX Authentication

Managing Cisco MSX Authentication contains the following sections:

About Password Policies

The password policies allow you to enforce secure password checks on newly created passwords for additional management users of the controller and access points.

Cisco MSX allows you to configure and update password policies using the Cisco MSX admin portal.

In Cisco MSX, you can define various settings for the password policies. These settings include password strength, password length, account locking, password history, and password aging.

By default, there are three built-in policies available on the Cisco MSX. As a user with an administrator role, you can modify these existing policies or create new policies. These built-in policies can be used when you add users. The default policies can be edited, but they cannot be deleted. The default policies created are:

- *ppolicy_default*: This policy applies to the consumer user.
- *ppolicy_strong*: This policy only applies to administrator accounts.
- *ppolicy_system*: This policy applies to both consumer and administrator accounts.

Configuring Password Policies

Using this procedure, you can configure password policies using the Cisco MSX portal.

Procedure

Step 1 Log in to the Cisco MSX portal using your credentials.

Step 2 From the left pane, choose **Settings** > **Authentication**.

The **Authentication** window is displayed.

Step 3 Click **Add Policy**.

Step 4 In the **Create Password Policy** window, enter the following details:

- In the **Password Policy** section, enter the details such as policy name, password history, password age, and password length.
- In the **Complexity Requirements** section, check the check boxes to include at least a number or a special character or an uppercase character or a lowercase character to make the password more complex.
- In the **Account Locking** section, check the **Enable** check box.

Step 5 Click **OK**.

A new policy is added and displayed in the Password Policies table.

Step 6 Select a policy from the Password Policies table and click **Edit** to change the password policy features.

Step 7 In the **Edit Password Policy** window, make the required changes, and click **OK**.

Deleting the Password Policy

a. Select a policy from the Password Policies table and click **Delete**.

b. In the **Delete Password Policy** window, click **Delete**.

Enabling Two-Factor User Authentication

Two-Factor Authentication (TFA) is an additional layer of security along with a strong password to ensure the identity of a user and reduce the risk of unauthorized access to Cisco MSX application and data. This additional factor can be something that only a user has access to, such as a One-time authentication code (OTP).

You can enable the Two-Factor Authentication from the Cisco MSX portal or by using the Global Settings API. To enable it from the Cisco MSX portal, select the **Use Two Factor Authentication** check box available in **Settings** > **Authentication**. For more information on the Global Setting API, refer to the Swagger documentation accessible from **Cisco MSX Portal** > **Account Settings** > **Swagger** > **Administration Service API**.

When enabled, it is applicable for all users. After the Two-Factor Authentication is enabled, users accessing the Cisco MSX portal must provide the following authentication factors:

- Username and password
- One-time authentication code (OTP). This code is sent to registered email address of the user. Each OTP is intended for use by only one user. This code is valid for a specific period of time and becomes invalid after the user successfully logs in.

By default, the user login attempts and validity duration of OTP are as follows:

- Number of user login attempts–The number of times a user can try logging in to the Cisco MSX portal. By default, this is five.
- Validity duration of OTP–The default validity duration of an OTP is 5 minutes. If the OTP expires, the user is forced to sign in again with the first authentication factor, that is, username and password.

Note

- Two-Factor Authentication is applicable only for web interface logins and not for REST API authentications.
- Two-Factor Authentication in web interface is not supported when Cisco MSX is configured with SAML Service.

Configuring Session Timeout Values

The Cisco MSX portal allows you to configure the inactivity timeout of a server session, as well as the absolute timeout.

Note

- Only an administrator user can modify the settings in the Settings area. These are system-wide timeouts that apply to all the users.
- Inactivity timeout defines how long the user session can last if the computer is idle or inactive for the configured amount of time. Whereas, absolute session timeout requires the user to log in again even if the user has been active the whole time.

When the session expires, Cisco MSX displays a message stating that the session has expired. You have the option to log in again or reauthenticate with the login credentials.

Using this procedure, you can configure session timeout values.

Procedure

Step 1 Log in to the Cisco MSX portal using your credentials.

Step 2 From the left pane, choose **Settings** > **Authentication**.

The **Authentication** window is displayed.

Step 3 In the session timeout, enter the inactivity timeout value and the absolute session timeout value in seconds.

Note

- Make sure that the inactivity timeout value is less than the absolute session timeout value.
- If you want to disable either one of these features, set the value to **-1**. Note that disabling these features is not recommended.

Step 4 Click **Save**.

Configuring Single Sign-On (SSO)

Cisco MSX allows you to configure and update SSO either through the API or the Cisco MSX admin portal.

Cisco MSX supports the following types of SSO configuration:

- **Configuring SAML-Based IDPs on Cisco MSX**: An Identity Provider (IDP) is responsible for issue authentication assertions. Cisco MSX can be configured with multiple SAML IDPs. If Service Providers already have one or more IDPs, they can configure Cisco MSX to work with these IDPs to set up SSO. Cisco MSX supports SAML 2.0 for SSO.

  When one or more IDPs are configured, Cisco MSX uses a subdomain to determine which IDP to route the login request to. The default IDP is the local database IDP—user credentials will be validated against the local user database. This means that by default, SSO using SAML is not enabled on Cisco MSX. Additional SAML IDP can be configured either through an API or through the Cisco MSX admin portal. Adding an IDP allows the login request to be routed to that IDP. Users will be logged in to Cisco MSX once the IDP authenticates the user.

- **Configuring the SSO Clients (Using Cisco MSX as an IDP)**: This means Cisco MSX can be configured as an IDP. Cisco MSX itself can also act as an IDP to other systems that want to use Cisco MSX for SSO. A third-party system can connect to Cisco MSX using OAuth2, OpendID Connect (OIDC), or SAML. SAML is an XML-based, open-standard data format that enables users to have access to multiple applications seamlessly after they sign in to Cisco MSX.

When a user visits the third-party system, they will be redirected to Cisco MSX to login. Once Cisco MSX authenticates the user, the user will be redirected back to the third-party system and is logged in there. These third-party systems are considered SSO clients to Cisco MSX. This can work in conjunction with the multiple IDPs configured in Cisco MSX.

This topic contains the following sections:

Configuring Single Sign-On (SSO) Through API

Cisco MSX enables you to configure and update SSO through API at run time. This will allow you to add and remove IDP, OAuth2 client, and SAML client without having to interact with consul directly. It will also not require a microservice restart.

Cisco MSX supports the following types of SSO authentication through API:

- **Configuring SAML-Based IDPs on Cisco MSX**: To configure Cisco MSX with multiple SAML IDPs, use the Identity Provider Management Controller section of the **User Management Service API**. For more information on the **User Management Service API**, refer to the Swagger documentation accessible from the **Cisco MSX portal** > **Account Settings** > **Swagger** > **User Management Service API**.
- **Configuring the SSO Clients (Using Cisco MSX as an IDP)**: To configure Cisco MSX as an IDP, use the Security Client Controller section of the **User Management Service API** if the SSO client is an Oauth2 or OpenID Connect (OIDC) client.

  If the SSO client is a SAML Service Provider, you need to additionally add the SAML specific details by using the SAML Service Provider Management Controller section of the **User Management Service API**. For more information on the **User Management Service API**, refer to the Swagger documentation accessible from the **Cisco MSX portal** > **Account Settings** > **Swagger** > **User Management Service API**.

Configuring Single Sign-On (SSO) Through the Cisco MSX Portal

In Cisco MSX, as a user with an administrator role, you can configure SSO using the Cisco MSX admin portal, in addition to using the API.

You need to either add the IDP or SSO clients based on your SSO requirements.

Cisco MSX supports the following types of SSO authentication through Cisco MSX Portal:

Configuring SAML-Based IDPs on Cisco MSX

Using this procedure, you configure the SAML based IDP using the Cisco MSX portal.

Procedure

Step 1 Log in to the Cisco MSX portal using your credentials.

Step 2 From the left pane, choose **Settings** > **SSO Configuration**.

The **SSO Configuration** window is displayed.

Step 3 Click the expand button for **Add IDP**.

A table appears with a list of all the IDPs that you can add, edit, or delete.

Step 4 Click **Add** to configure Cisco MSX with one SAML IDP.

The **Add IDP** window is displayed.

Step 5 Enter the following in the **Domain** section.

- Enter the **Domain Name**
- Select the **Type** from the drop-down list

Step 6 Enter the following in the **Identification** section.

- Entity ID
- External ID Name
- External IDP Name

Step 7 Enter the following in the **Security** section.

- Enter the **Metadata**
- Enter the **Failure URL**
- Check the **Require Signature** check box
- Check the **Require Trust Check** check box
- Enter the **Trusted Keys**

Note Click + if you want to enter multiple trusted keys.

Step 8 Create a tenant dynamically by enabling **Create User** option.

To create a tenant:

a) Check the **Create User** checkbox to create a tenant (federated user) based on the SAML assertion, if the user does not exist already.

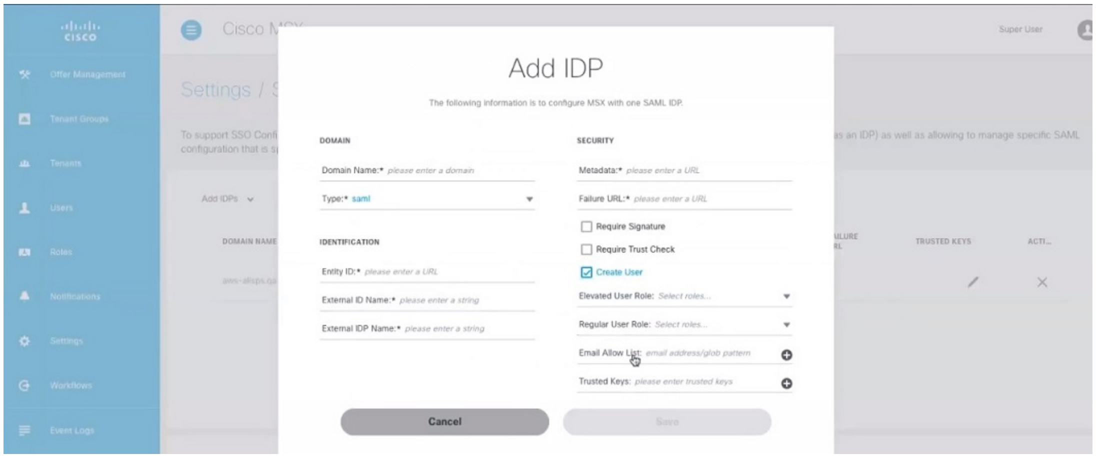
Note For more information on the dynamic tenant creation, see Generating Tenant Dynamically from Cisco.com Account.

b) Click any one of the following field to further define the create user functionality or roles.

- **Elevated User Roles**: Roles assigned to the first user, who is dynamically created as tenant.
- **Regular User Roles**: Roles assigned to the other users created under the tenant (federated user).
- **Email Allow List**: Allowed list restricts the user who can be auto created or updated from this IDP. If the allowed list is defined, only user that matches the allowed list can be auto created or updated in Cisco MSX. Each item in the allowed list will be used to match the email attribute in the assertion. The allowed list can contain exact match that is either the exact email address or just the email domain (@Cisco.com) to match all the email address from Cisco.com.

Note If the allowed list is not defined, any user from the IDP will be auto created or updated in Cisco MSX.

Figure 1: Create User



Add IDP

The following information is to configure MSX with one SAML IDP.

DOMAIN

Domain Name:* please enter a domain

Type:* saml

IDENTIFICATION

Entity ID:* please enter a URL

External ID Name:* please enter a string

External IDP Name:* please enter a string

SECURITY

Metadata:* please enter a URL

Failure URL:* please enter a URL

☐ Require Signature

☐ Require Trust Check

☑ Create User

Elevated User Role: Select roles...

Regular User Role: Select roles...

Email Allow List: email address/glob pattern

Trusted Keys: please enter trusted keys

Step 9 Click **Save**.

A new IDP is added and displayed in the IDPs table.

Step 10 Select an IDP from the IDPs table, click the **Edit** icon if you want to change the IDP features.

The **Edit IDP** window is displayed.

Step 11 Change the features as required and click **Save**.

Step 12 Select an IDP from the IDPs table, click the **Delete** icon if you want to delete an IDP.

The **Delete IDP** window is displayed.

Step 13 Click **Delete**.

Configuring Single Sign-On (SSO) Using Cisco MSX as an IDP

Cisco MSX allows you to configure SSO using Cisco MSX as an IDP in the Cisco MSX admin portal.

The SSO clients are of two types—SAML and Non-SAML. It depends on the selection of the value in the **Grant Types** field selection.

Configuring the Non-SAML SSO Client

Using this procedure, you can configure SSO using the Cisco MSX portal for non-SAML SSO client authentication.

Procedure

Step 1 Log in to the Cisco MSX portal using your credentials.

Step 2 From the left pane, choose **Settings** > **SSO Configuration**.

The **SSO Configuration** window is displayed.

Step 3 Click the expand button for **Add SSO Clients**.

A table is displayed with a list of all the SSO Clients that you can add, edit, or delete.

Step 4 Click **Add** to configure Cisco MSX with non-SAML SSO Client.

The **Add SSO Client** window is displayed.

Step 5 In the **Attributes** section:

- Select the **Grant Types** from the drop-down list.

  Note
  - Based on the **Grant Types** value you select, you can either select the SAML Authentication or non-SAML Authentication.
  - Select anything from the **Grant Types** drop-down list except for SAML2 bearer for non-SAML authentication.

    For example, if you select anything from the Grant Types drop-down list apart from *urn:ietf:params:oauth:grant-type:saml2-bearer*, it is a non-SAML authentication.

- Enter the **Additional information**
- Click **Yes/No** radio button next to the **Use Session Timeout**
- Enter the **Registered Redirect URLs**
- Enter nfv-api to the **Resource IDs**

  Note *nfv-api* is the only valid resource ID value accepted right now.

Step 6 In the **Token** section, enter:

- Access Token Validity Seconds
- Max Tokens Per User
- Refresh Token Validity Seconds

Step 7 In the **Client ID** section, enter:

- Client ID
- Client Secret

Note In the case of Cisco SD-WAN, specify the IP Address of the SD-WAN Control Plane.

Step 8 In the **Scope** section, enter:

- Scopes
- Auto Approve Scopes

Step 9 Click **Save**.

A new SSO Client configuration is added and displayed in the SSO Clients table.

Step 10 Select a SSO Client from the SSO Clients table, click the **Edit** icon if you want to change the SSO Client features.

Note The Client Security is displayed with **********. Do not change its value to save the SSO Client, which means that the existing value will be used.

The **Edit SSO Client** window is displayed.

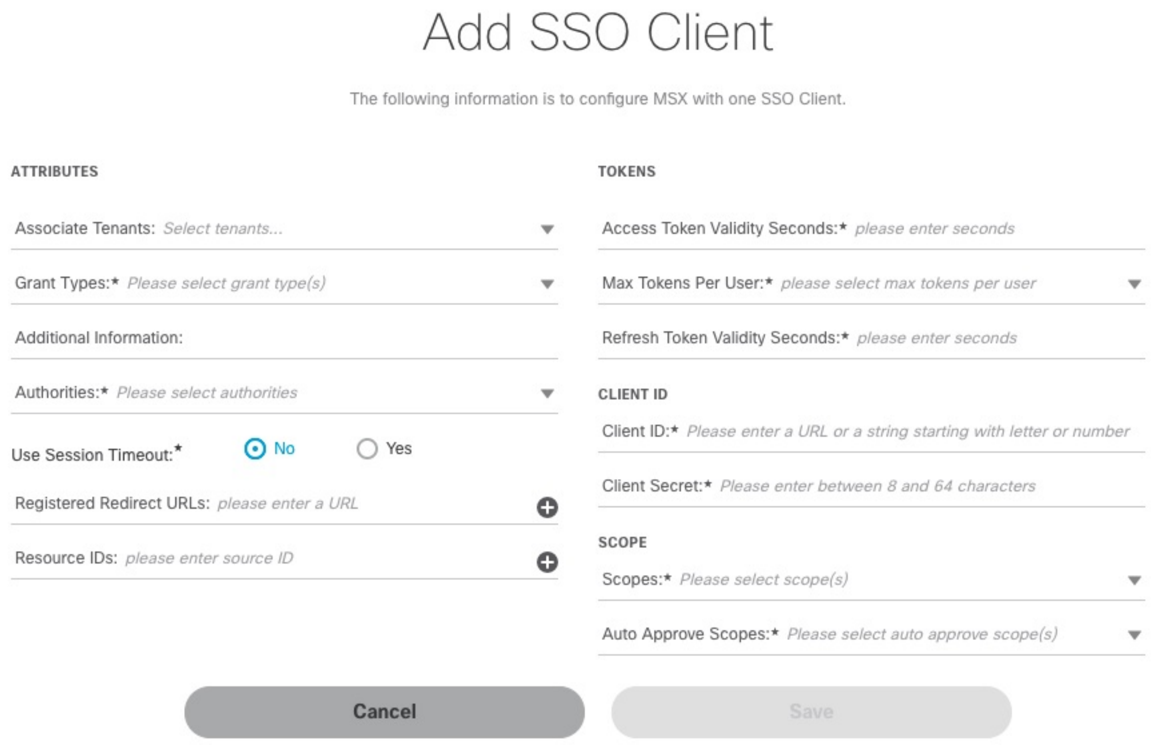
Step 11 Change the features as required and click **Save**.

Step 12 Select a SSO Client from the SSO Clients table, click the **Delete** icon if you want to delete a SSO Client.

The **Delete SSO Client** window is displayed.

Step 13 Click **Delete**.

Figure 2: Add SSO Client Window



Add SSO Client

The following information is to configure MSX with one SSO Client.

ATTRIBUTES

Associate Tenants: *Select tenants...*

Grant Types:* *Please select grant type(s)*

Additional Information:

Authorities:* *Please select authorities*

Use Session Timeout:* ● No ○ Yes

Registered Redirect URLs: *please enter a URL*

Resource IDs: *please enter source ID*

TOKENS

Access Token Validity Seconds:* *please enter seconds*

Max Tokens Per User:* *please select max tokens per user*

Refresh Token Validity Seconds:* *please enter seconds*

CLIENT ID

Client ID:* *Please enter a URL or a string starting with letter or number*

Client Secret:* *Please enter between 8 and 64 characters*

SCOPE

Scopes:* *Please select scope(s)*

Auto Approve Scopes:* *Please select auto approve scope(s)*

What to do next

Applicable only for Cisco SD-WAN users (For Cisco SD-WAN-specific SSO Configuration).

For SSO to seamlessly work between Cisco MSX to SD-WAN Control Plane, do the following additional steps:

1. Upload the Cisco MSX Metadata to SD-WAN Control Plane.
   a. Download the Cisco MSX metadata from the following link: https://msx-fqdn/idm/metadata.
   b. Upload the metadata file to SD-WAN Control Plane manually using the SD-WAN Control Plane web interface under Settings > Identity Provider Settings.
2. Create user roles in Cisco MSX that map to SD-WAN Control Plane user roles (Basic, Netadmin, and Operator).

Configuring the SAML SSO Client

Using this procedure, you can configure SSO using the Cisco MSX portal for SAML SSO client authentication.

Procedure

Step 1 Log in to the Cisco MSX portal using your credentials.

Step 2 From the left pane, choose **Settings** > **SSO Configuration**.

The **SSO Configuration** window is displayed.

Step 3 Click the expand button for **Add SSO Clients**.

A table is displayed with a list of all the SSO Clients that you can add, edit, or delete.

Step 4 Click **Add** to configure Cisco MSX with SAML SSO Client.

The **Add SSO Client** window is displayed.

Step 5 In the **Attributes** section:

- Select the **Grant Types** from the drop-down list.

  Note
  - Based on the **Grant Types** value you select, you can either select the SAML Authentication or non-SAML Authentication.
  - Select **SAML2 bearer** for SAML authentication from the **Grant Types** drop-down list.

    For example, if you select *urn:ietf:params:oauth:grant-type:saml2-bearer* from the Grant Types drop-down list, it is a SAML authentication.

- Enter the **Metadata Source**.

  Note You need to enter the Metadata Source details if you select SAML authentication, which is not required for non-SAML authentication.

  - Check the **Require Metadata Signature** box
  - Check the **Require Metadata Trust** box

- Enter the **Security Profile**
- Enter the **Metadata Trusted Keys**

  Note Click **+** if you want to enter multiple trusted keys.

- Enter the **Additional information**
- Click **Yes/No** radio button next to the **Use Session Timeout**
- Enter the **Registered Redirect URLs**
- Enter the **Resource IDs**

Step 6 In the **Token** section, enter:

- Access Token Validity Seconds

- Max Tokens Per User
- Refresh Token Validity Seconds

Step 7 In the **Client ID** section, enter:

- Client ID
- Client Secret

Note In the case of Cisco SD-WAN, specify the IP Address of the SD-WAN Control Plane.

Step 8 In the **Scope** section, enter:

- Scopes
- Auto Approve Scopes

Step 9 Click **Save**.

A new SSO Client configuration is added and displayed in the SSO Clients table.

Step 10 Select a SSO Client from the SSO Clients table, click the **Edit** icon if you want to change the SSO Client features.

Note The Client Security is displayed with **********. Do not change its value to save the SSO Client, which means that the existing value will be used.

The **Edit SSO Client** window is displayed.

Step 11 Change the features as required and click **Save**.

Step 12 Select a SSO Client from the SSO Clients table, click the **Delete** icon if you want to delete a SSO Client.

The **Delete SSO Client** window is displayed.

Step 13 Click **Delete**.

What to do next

Applicable only for Cisco SD-WAN users (For Cisco SD-WAN-specific SSO Configuration).

For SSO to seamlessly work between Cisco MSX to SD-WAN Control Plane, do the following additional steps:

1. Upload the Cisco MSX Metadata to SD-WAN Control Plane.
   a. Download the Cisco MSX metadata from the following link: https://msx-fqdn/idm/metadata.
   b. Upload the metadata file to SD-WAN Control Plane manually using the SD-WAN Control Plane web interface under Settings > Identity Provider Settings.
2. Create user roles in Cisco MSX that map to SD-WAN Control Plane user roles (Basic, Netadmin, and Operator).

Configuring SSO for Meraki Using Cisco MSX as an IDP

Cisco MSX IDP-initiated SSO allows you to access Meraki dashboard from Cisco MSX. Using this procedure, you can configure SSO for Meraki using Cisco MSX as an IDP.

Procedure

Step 1 Configure the following on Meraki side:

a) Download the Cisco MSX metadata from the following link: https://msx-fqdn/idm/metadata.

b) Configure the SAML Single Sign-on for Dashboard. Perform the Dashboard Configuration tasks mentioned in Meraki Documentation here .

Note

- Instead of uploading a metadata file, Meraki requires you to provide an **X.509 cert SHA1 fingerprint**. The x509 certificate is included in the metadata file downloaded in step a. You can use any suitable tool to generate the fingerprint. Meraki documentation shows how to do it using a Windows machine. If you are using a Mac machine, you can use the **openssl** command to generate the fingerprint. For more information, see Generating X509 Fingerprint from Metadata File on Mac, on page 12.
- The name of the SAML role should be the same as in Cisco MSX.

Step 2 After you complete the above steps, configure the following on Cisco MSX side:

a) Create a metadata file to use in Cisco MSX because Meraki does not provide a metadata file. Use the following as a template and replace the **validUntil** attribute as appropriate. Use https://dashboard.meraki.com as the **entityID** when the tenancy model uses a shared set of meraki organizations. You can generate an **entityID** in the format "<organization-id > -meraki-entity" when you have a service provider model and have multiple customers from unrelated organizations. In **AssertionConsumerService.Location** field, add the Consumer URL from Meraki Dashboard. For more information, see the section *IdP Attribute Information* in the Meraki Documentation.

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2021-11-12T16:48:56.423Z"
 entityID=\"<entity-id>\">
  <SPSSODescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
validUntil="2021-11-12T16:48:56.422944Z"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" AuthnRequestsSigned="false"
WantAssertionsSigned="true">
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location=\"<consumer-URL-from-organization>\" index="0" isDefault="true"></AssertionConsumerService>

  </SPSSODescriptor>
</EntityDescriptor>
```

Note You must use the same SAML role for all organizations with SSO enabled to use the Consumer URL of any organization in metadata.

b) Use the metadata file in Cisco MSX. For more information, see Configuring SAML-Based IDPs on Cisco MSX, on page 5.

Step 3 Add a link similar to the following in Cisco MSX to trigger the Cisco MSX IDP-initiated SSO.

```
http://<msxsystem>:8765/idm/v2/authorize?entity_id=https%3A%2F%2Fdashboard.meraki.com&
grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Asaml2-bearer&idp_init=true
```

In the above link, **entity_id** points to the Meraki SAML **entityID** you used in step 2.a, on page 12. The **idp_init** parameter tells Cisco MSX to initiate the SSO process from the Cisco MSX side.

Generating X509 Fingerprint from Metadata File on Mac

Using the procedure, you can generate X509 fingerprint from a metadata file on Mac.

Procedure

Step 1 Copy the <X509Certificate> used for signing from the metadata file and save it in a temp file. For instance, tmp.txt.

Step 2 Use the following command to format the temp file to 64 characters per line:

```
sed -e "s/.\{64\}/&\r/g" < tmp.txt > idp.crt
```

Step 3 Open the idp.crt file and add **-----BEGIN CERTIFICATE-----** as the first line of the file and **-----END CERTIFICATE-----** as the last line:

```
-----BEGIN CERTIFICATE-----
<CERTIFICATE-CONTENT-HERE>
-----END CERTIFICATE-----
```

Step 4 Use the **openssl** command to generate the finger print:

```
openssl x509 -noout -fingerprint -in idp.crt
```

Retrieving the Device Password

The Cisco MSX platform allows you to retrieve the deleted or existing device password using the serial number. When the devices are deleted from the Cisco MSX, you can enter the device serial number in the **Devices** window and retrieve the deleted device password using the **IDM Microservice** API.

You can manage the configurations of the **IDM Microservice** API as follows:

Manage the secrets configuration and supports scope such as servicetype, devicetype, devicesubtype, and serialkey. Use the **Secrets Controller** API of the **IDM Microservice** API.

For more information on this API, refer to the Swagger documentation that can be accessed for **Cisco MSX portal** > **Account Settings** > **Swagger** > **IDM Microservice API**.

Using this procedure, you can retrieve the deleted password using the device serial number.

Procedure

Step 1 Log in to the Cisco MSX portal using your credentials.

Step 2 From the left pane, click **Devices**.

The **Devices** window is displayed.

Step 3 Click the **ellipsis (...)** that is located on the far right of the column heading and choose **Retrieve Deleted Device**.

The **Retrieve Deleted Device** dialog box is displayed.

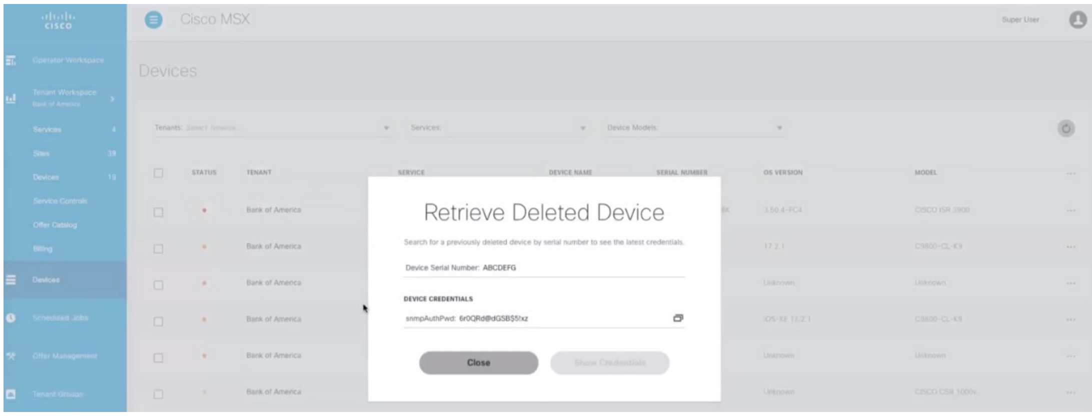
You can also select mutliple device and click the **ellipsis (...)** on the column heading to retrieve multiple deleted devices credential.

Step 4 Enter the device serial number.

Step 5 Click **Show Credentials**.

The device credential is displayed. You can also copy this device password by clicking the **Copy** icon.

Figure 3: Retrieve Deleted Device



Retrieve Deleted Device

Search for a previously deleted device by serial number to see the latest credentials.

Device Serial Number: ABCDEFG

DEVICE CREDENTIALS

snmpAuthPwd: 6r0QRd@dGSB$5!xz

Back

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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