Commerce API – Migration

Table of Contents

[Preface 2](#_Toc122031688)

[What’s Changing? 2](#_Toc122031689)

[What’s not Changing? 2](#_Toc122031690)

[Migration Steps 3](#_Toc122031691)

[1. Register new Client Application 3](#_Toc122031692)

[Mashery API Console: 3](#_Toc122031693)

[Mule API Console: 5](#_Toc122031694)

[2 Change your application component for Token creation 9](#_Toc122031695)

[3 Change your application component for runtime API invocation 10](#_Toc122031696)

[Clean Up 10](#_Toc122031697)

[Support 11](#_Toc122031698)

[FAQ 12](#_Toc122031699)

[When do I start migrating my applications? 12](#_Toc122031700)

[Who do I contact if I run into issues? 12](#_Toc122031701)

[My application is developed & supported by a 3rd party company. Can they do this work? 12](#_Toc122031702)

[Does this impact production and Partner Onboarding Environment (POE)? 12](#_Toc122031703)

[By when will by existing applications stop working in production? 12](#_Toc122031704)

[Are there any exception processes at this time? 12](#_Toc122031705)

[URL 13](#_Toc122031706)

[Mashery: 13](#_Toc122031707)

[Mashery API Console: 13](#_Toc122031708)

[Mashery Token URL: 13](#_Toc122031709)

[Mashery Runtime host: 13](#_Toc122031710)

[MuleSoft: 13](#_Toc122031711)

[MuleSoft API Console: 13](#_Toc122031712)

[MuleSoft Token URL: 13](#_Toc122031713)

[MuleSoft Runtime Host: 13](#_Toc122031714)

# Preface

The purpose of this document is to document the steps required to successfully migrate your registered applications on CISCO API Portals for commerce APIs so they continue to operate without disruption in a much more secure platform as well as to offer more choices for subscribing to newer APIs in the future.

## What’s Changing?

1. Cisco is migrating from PingIdentity to Okta
2. Okta offers better security strategies and a more secure platform. Certain OAuth grant types will cease to be supported as we continue this journey
3. Authentication URLs, request/responses, run-time URLs (as applicable) will be changed
4. New APIs cannot be added to your existing registered applications
5. Your existing token generation URLs will not work
6. OAuth Ping tokens will be changing to JWT tokens.
7. On Mashery API Console (apiconsole.cisco.com) you must selection application type and appropriate / allowed OAuth grant type for new application registration.
8. In some cases, underlying gateway platforms may also migrate to a higher version
9. Your existing applications will cease to work (token generation errors) after 02-Apr-2023

## What’s not Changing?

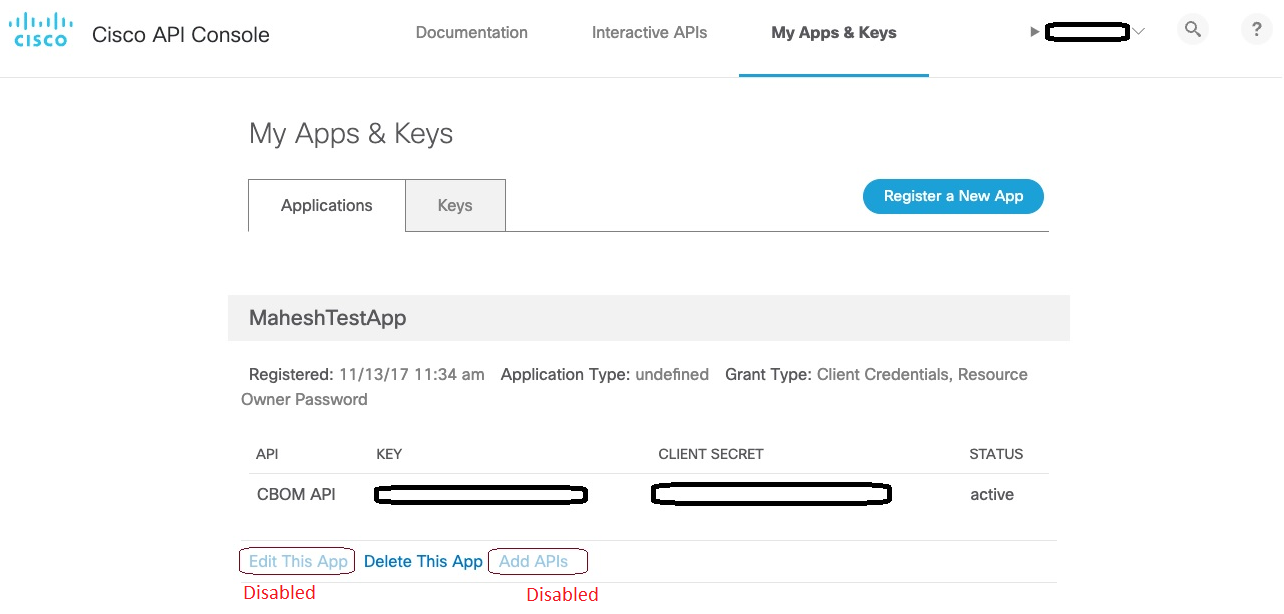
1. As part of Cisco’s initiative to move from PingIdentity to Okta, API functionalities are not changed. However, functional changes do occur on APIs on an ongoing basis to meet subscriber demands.
2. Server certificates, supported encryption algorithms & protocols are not expected to change but do expect changes in future. Please do check your trust store and ensure compatibility with new URLs and certificates associated.
3. No runtime impact on current applications until the cutover date of 02-Apr-2023

# Migration Steps

## Register new Client Application

### Mashery API Console:

* 1. Logon to apiconsole.cisco.com
  2. Make a note of the existing application and its subscribed list of APIs as shown below.



1.3 Click on “Register a new App” button and fill out the application details. An example of a filled-out form is shown for example only. Please note the Application type is newly introduced to help you to select the best possible OAuth grant type. Resource Owner Password Credentials grant type is subject to deprecation and is highly recommended not to be used although this option is available for selection under “Native” application temporarily and is usable until OAuth 2.1 specification is approved.

Graphical user interface, text, application, email

Description automatically generated

NOTE: Certain recommended OAuth grant types for the selected application type are preselected for you and cannot be unselected. In the above example Authorization code grant type is preselected and cannot be unselected and hence warrants a mandatory callback (Redirect URI) to be provided. Please refer to [OAuth 2.0 Specification](https://oauth.net/2/) and [API Console Documentation](https://apiconsole.cisco.com/docs/read/overview/Oauth_20_Topics) for OAuth 2.0 for additional information.

Graphical user interface, text, application

Description automatically generated Graphical user interface, text, application

Description automatically generated

* 1. Please agree to the terms of service and click on Register.
  2. Confirm successful registration of the application. Congratulations you have completed Application registration.

Graphical user interface, text, application, email

Description automatically generated

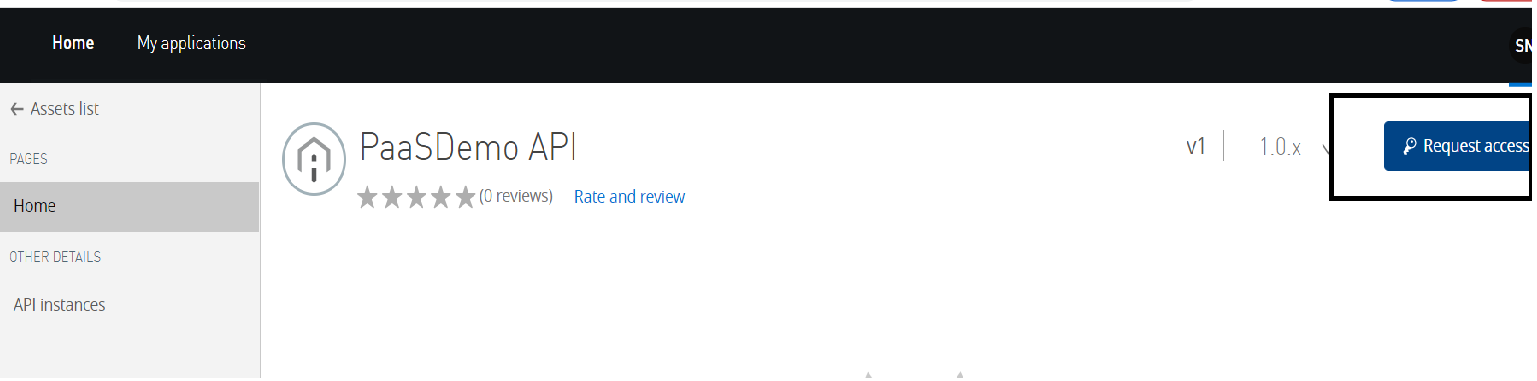
### Mule API Console:

1.1.1 Login to the MuleSoft developer portal using Cisco SSO with below links

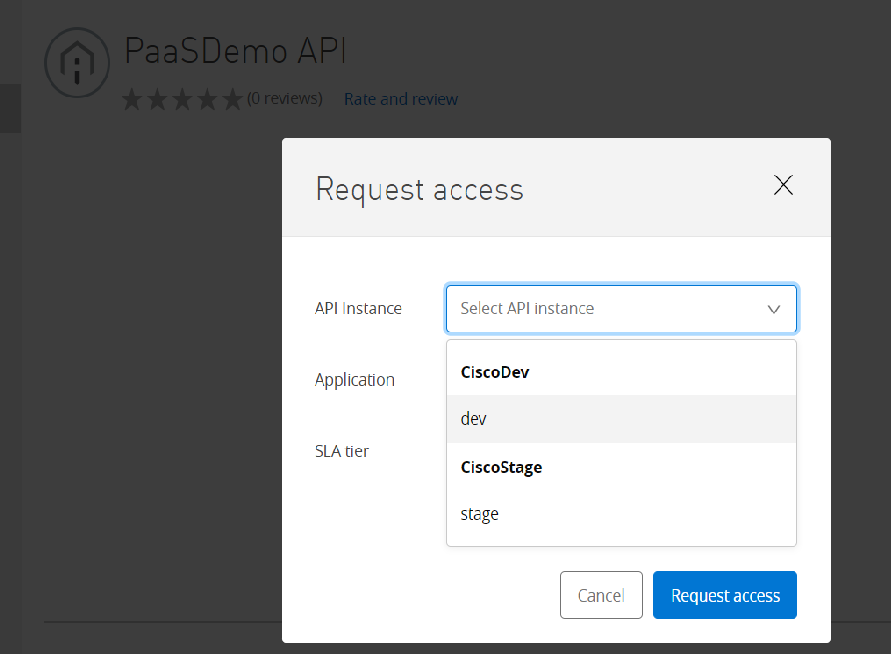
* NPRD: <https://anypoint.mulesoft.com/exchange/portals/cisco-nprod>
* PROD: <https://anypoint.mulesoft.com/exchange/portals/cisco-prod>

1.1.2 OAuth Client application creation steps.

* Select the API asset to which you want to request access.
* In the API asset page click on the version to which you need access and then click on "Request access" button on top right corner as shown below.



1.1.3 From the API Instance drop down, select the API Instance to which you want to request access.



* + 1. Once the instance is selected then select "Create a new application" option from the Application dropdown as shown below.

Graphical user interface, text, application

Description automatically generated

* + 1. In the next tab, enter application name, description, application URL, and select the OAuth grant type based on your application use case and click create button, once the create button is clicked platform will go ahead and create the client application with chosen grant type in Client Provider and you will get the required clientID and clientSecret details.

Graphical user interface, text, application, email

Description automatically generated

* + 1. Next, if any SLA tier is defined for the API then select the appropriate SLA tier from dropdown list and click on "Request" button to request API access to the OAuth client application you have created in step #1.1.5.

Graphical user interface

Description automatically generated

* + 1. Based on the API access request approval flow, your request will be reviewed by API owner and will be approved. If its an auto approval then you API request access will be automatically approved, and you can use the client application to access the API instances.

## Change your application component for Token creation

* 1. Upon successful completion of your application registration, you should have received an email with your keys (client id and client secret). If you did not, you can always go to “My apps and Keys” menu and look for the keys associated with the newly registered application.
  2. Use this for the token generation.
  3. A Simple client\_credential grant type invocation via Postman desktop application shown below for your convenience. Notice the URL change and the response structure change as well as the JWT token which is much longer than the previously issued Ping tokens.

Graphical user interface, text, application

Description automatically generated

## Change your application component for runtime API invocation

# Clean Up

1. Once you are satisfied with newly registered client application, please delete your older application.

# Support

If your existing application authentication works but the newly registered application fails to create tokens, please reach out to apix-support(mailer list) at [apix-support@cisco.com](mailto:apix-support@cisco.com) and for MuleSoft related APIs please reach out to apm-support@cisco.com at [apm-support@cisco.com](mailto:apm-support@cisco.com)

# FAQ

## When do I start migrating my applications?

You can start after 15-Jan-2023.

## Who do I contact if I run into issues?

Please refer to the support section of this document

## My application is developed & supported by a 3rd party company. Can they do this work?

Yes, some 3rd party companies own the application registration on behalf of you while most are registered and owned by your company and its credentials (client ID and Secret) and connection information is shared with the 3rd party.

## Does this impact production and Partner Onboarding Environment (POE)?

Yes, it impacts all production and non-production Cisco and associated client (your) application environments

## By when will by existing applications stop working in production?

02-Apr-2023

## Are there any exception processes at this time?

None. It is in the best interest of all the API connected eco system that Cisco is endeavoring to improve. Cisco wants to offer the most secure connectivity possible to its partners to do business.

# URL

## Mashery:

### Mashery API Console:

Existing: apiconsole.cisco.com

New: apiconsole.cisco.com

Comment: No Change. Okta enablement is done on 15-Jan-2023 which replaces PingIdentity portal.

### Mashery Token URL:

Existing: <https://cloudsso.cisco.com/as/token.oauth2>

New: <https://id.cisco.com/oauth2/default/v1/token>

### Mashery Runtime host:

Existing: api.cisco.com

New: apix.cisco.com

Comment: Host name changes, however certificates, IP addresses remain the same. Host alias added to existing certificate. API context path remains the same unless specifically called out.

## MuleSoft:

### MuleSoft API Console:

Existing: <https://anypoint.mulesoft.com/apiplatform/apx/#/portals>

New: <https://anypoint.mulesoft.com/exchange/portals/cisco-prod>

### MuleSoft Token URL:

Existing: <https://cloudsso.cisco.com/as/token.oauth2>

New: <https://id.cisco.com/oauth2/default/v1/token>

### MuleSoft Runtime Host:

Existing: apx.cisco.com/commerce/…/v1/api

New: apx.cisco.com/commerce/…/v2/api

Comment: Version upgrade and hence v\* in the context path will change. Host name remains the same.