



Overview: Milestone Draft (Cisco Internal)

[Cisco MSX Platform Overview](#) 2

[What's New in Cisco MSX Platform](#) 2

[Audience](#) 2

[Logging In and Logging Out of the Cisco MSX Portal](#) 3

[Accessing Cisco MSX APIs](#) 3

[About this Content](#) 4

Revised: May 20, 2022

[← Back](#)

Cisco MSX Platform Overview

Cisco MSX is an open software platform that enables service providers to create and manage services across physical and virtual network elements. The Cisco MSX solution utilizes network function virtualization and enables service providers to provide their customers a flexible selection of services that are easily customized through a self-service portal. It reduces the costs for service creation, customer acquisition, service fulfillment, time to repair, and maintenance. With Cisco MSX solution, you can automate end-to-end provisioning for different use cases and service topologies. Each release of the Cisco MSX provides out-of-box capabilities to orchestrate particular use cases, also called service packs (such as, Cisco MSX SD-WAN, Cisco MSX SD-Branch, and Cisco MSX Managed Devices). The Cisco MSX service packs are a suite of prepackaged software capabilities that fully automate the end-to-end service creation including ordering, service chaining, orchestration, service assurance, user self care, real time performance reporting, and user-defined policy changes. With these fully validated service level packages, end customers can quickly turn on, control, and ensure cloud-based managed services offered by the service provider. For more information about Cisco MSX solution, see [Cisco Managed Services Accelerator \(MSX\) 4.3 Solution Overview Documentation](#).

What's New in Cisco MSX Platform

Feature	Description
Account Locking Using Password Policies	Cisco MSX portal allows you to enable lockout of a user account using password policies. For more information, see Configuring Password Policies Through the Cisco MSX Portal .
Configuring Webhooks	Cisco MSX allows you to receive notifications when changes are made to a third-party system through webhooks. For more information, see Configuring Webhooks .
Configuring API Keys	Cisco MSX provides API keys to enable access to specific APIs. The API keys do not specifically represent a tenant or user; instead, they function as an additional layer of security on top of the Cisco MSX authentication system. For more information, see Configuring API Keys .

Audience

This guide is designed for administrators who use Cisco MSX platform to configure basic operations after installing Cisco MSX. The platform addendum should be used in conjunction with this guide.

Logging In and Logging Out of the Cisco MSX Portal

To log into the Cisco MSX portal, enter the following URL in your web browser address field, where server-ip is the IP address or fully qualified domain name (FQDN) name of the Cisco MSX server:

https://<server-ip>/vms or https://<your_portal_fqdn>

Depending on your network configuration, the first time your browser connects to the Cisco MSX web server, you may have to update your client browser to trust the security certificate of the server. This ensures the security of the connection between your client and the Cisco MSX web server.

Your user account privileges determine what you can see and do in the user interface. For information on Cisco MSX users and the actions they can perform, see [Managing User Roles](#).

If you are using any third-party applications with Cisco MSX, you can configure single-sign on (SSO) to access these applications from Cisco MSX. For more information about configuring single-sign on, see [Configuring Single Sign-On](#).

To log out, in the left pane of the Cisco MSX portal, click **Logout**.

Accessing Cisco MSX APIs

In Cisco MSX, OAuth 2.0 access tokens are used to make API requests to the application on behalf of a user. After the user is authenticated using the Cisco MSX credentials, they can obtain the access token which is shown in the procedure below. The same token can be used on each API request to indicate the request is executed on behalf of the user.

Using this procedure, you can use the Cisco MSX APIs for platform or service-pack operations.

Procedure

Step 1 Obtain the Cisco MSX client credentials.

Use the credential for logging in to the Cisco MSX portal. If you do not have these credentials, contact your Service Provider Administrator.

Step 2 Obtain an access token from the Cisco MSX authorization Server.

Use the following curl command to get the token.

```
curl -k -d 'grant_type=password&username=*****&password=*****' -H "Content-Type: application/x-www-form-urlencoded" -H "Authorization: Basic *****" -X POST https://<Product_URL>/idm/v2/token
```

Step 3 Send the access token to an API.

After obtaining the access token, send the token to an Cisco MSX API in an HTTP authorization header. The below example shows a sample curl command for updating the current password policies. Use the access_token that was obtained in Step 2 to run this curl command.

```
curl -k -X PUT --header "Content-type: application/json" --header "accept: application/json" --header "authorization: Bearer <ACCESS_TOKEN>" -d '{ "accountLocking": { "enabled": true, "lockoutDurationMin": 30, "lockoutFailCount": 3, "lockoutFailIntervalSec": 60 }, "agingRule": { "enabled": true, "expireWarningSec": 1209600, "graceAuthNLimit": 3, "maxAgeSec": 0, "minAgeSec": 0 }, "characterRule": { "enabled": true, "minDigit": 1, "minLowercasechars": 1, "minSpecialchars": 0, "minUppercasechars": 1 }, "description": "string", "historyRule": { "enabled": true, "passwdhistorycount": 10, "passwdhistorydurationMonth": 60 }, "lengthRule": { "enabled":
```

```
true, "maxLength": 16, "minLength": 8 }, "name": "ppolicy_default" }'  
https://<Product_URL>/idm/api/v1/pwdpolicy/ppolicy_default
```

Your client application requests an access token from the Cisco MSX authorization server, extracts a token from the response, and sends the token to the Cisco MSX API that you want to access.

About this Content

This section provides information about related documentation of Cisco MSX and trademarks used in this content.

Related Documentation

You can access Cisco MSX 4.3.0 content at [Cisco MSX End User Documentation](#).

The documents listed here are available for additional reference. To access API documentation on the Swagger GUI, log in to the Cisco MSX GUI and navigate to **My Profile > Swagger API**.

Cisco MSX SDK documentation is available at <https://developer.cisco.com/site/msx/>.

Document	Description
Cisco Managed Services Accelerator (MSX) 4.3 Release Notes Documentation	This documentation provides information about the new features in Cisco MSX 4.3.
Cisco Managed Services Accelerator (MSX) 4.3 Administration Documentation	This documentation covers the post-install configuration information that is required to set up Cisco MSX.
Cisco Managed Services Accelerator (MSX) 4.3 Platform and Service Pack Permissions Addendum	This addendum covers all the permissions that are required to operate Cisco MSX and the service packs.
Cisco Managed Services Accelerator (MSX) 4.3 SD-WAN Service Pack Documentation	This documentation includes details that are related to deploying, managing, configuring the Cisco MSX SD-WAN service pack, and troubleshooting service errors.
Cisco Managed Services Accelerator (MSX) 4.3 SD-WAN Out-of-the-Box Applications Addendum	This document is an addendum to the <i>Cisco MSX SD-WAN Service Pack</i> content. It has details about the out-of-the-box applications of Cisco MSX 4.3 and the comparison of applications in older releases with applications in Cisco MSX 4.3 based on possible application mapping.
Cisco Managed Services Accelerator (MSX) 4.3 Enterprise Access Service Pack Documentation	This documentation includes details that are related to deploying, managing, configuring the Cisco MSX Enterprise Access service pack, and troubleshooting service errors.
Cisco Managed Services Accelerator (MSX) 4.3 Managed Device Service Pack Documentation	This documentation includes details related to subscribing the Cisco MSX Managed Device service pack, configuring the service, and troubleshooting service errors.
Cisco Managed Services Accelerator (MSX) 4.3 Solution Overview Documentation	This documentation provides a comprehensive explanation of the design of the Cisco MSX solution that enables service providers to offer flexible and extensible services to their business customers.

Document	Description
Open Source Used in Cisco MSX and Service Packs Documentation	This documentation contains licenses and notices for Open Source software that is used in this product.

Bias-free Doc Disclaimer



Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in

the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

 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.