Overview

Revised: September 17, 2021

Cisco Managed Services Accelerator (MSX) Platform Overview

Cisco Managed Services Accelerator (MSX) is an open software platform that enables service providers to create and manage services across physical and virtual network elements. The 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 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 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 MSX solution, see Cisco Managed Services Accelerator (MSX) Solution Overview.

What's New in Cisco MSX Platform

Feature	Description
Configuration Change Management Approvals	MSX platform provides an approval process for configuration change requests made by a user. If there is a change request on MSX, the request (which includes the Entity ID, Entity CR date, Context source path, and url) is forwarded to ServiceNow through the Change Request service.

Audience

This guide is designed for administrators who use Cisco MSX platform to configure basic operations after installing MSX.

The platform addendum should be used in conjunction with this guide.

Logging In and Logging Out of the MSX Portal

To log into the 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 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 MSX, you can configure single-sign on (SSO) to access these applications from MSX. For more information about configuring single-sign on, see Configuring Single Sign-On.

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

Accessing 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 MSX APIs for platform or service-pack operations.

Before you begin

Configure authorization server (Auth Server) properties. For more information, see Configuring Authorization Server Properties.

Procedure

Step 1 Obtain the MSX client credentials.

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

Step 2 Obtain an access token from the 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://<MSX_URL>/idm/v2/token
```

Step 3 Send the access token to an API.

After obtaining the access token, send the token to an 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://<MSX_URL>/idm/api/v1/pwdpolicy/ppolicy_default
```

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

Related Documentation

You can access Cisco MSX 4.1 content at https://www.cisco.com/c/en/us/td/docs/net_mgmt/msx/end_user_doc/4_1/Cisco_MSX_End_User_Documentation.html.

The documents listed here are available for additional reference. To access API documentation on the Swagger GUI, log in to the 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) 4.1 Release Notes	This documentation provides information about the new features in Cisco Managed Services Accelerator (MSX) 4.1.
Cisco Managed Services Accelerator (MSX) 4.1 Administration	This documentation covers the post-install configuration information that is required to set up MSX.
Cisco Managed Services Accelerator (MSX) 4.1 Platform and Service Pack Permissions Addendum	This addendum covers all the permissions that are required to operate MSX and the service packs.
Cisco Managed Services Accelerator(MSX) 4.1 SD-WAN	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) 4.1 SD-WAN and Meraki Out-of-the-Box Applications Addendum	This document is an addendum to the *Cisco MSX SD-WAN Service Pack* content. It has details about the out-of-the-box applications of MSX 4.1 and the comparison of applications in older releases with applications in MSX 4.1 based on possible application mapping.
Cisco Managed Services Accelerator (MSX) 4.1 Enterprise Access	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) Solution Overview	This documentation provides a comprehensive explanation of the design of the MSX solution that enables service providers to offer flexible and extensible services to their business customers.
Open Source Used in Cisco MSX and Service Packs	This documentation contains licenses and notices for Open Source software that is used in this product.

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.