Overview

Revised: September 16, 2021

Audience

This guide is designed for service provider operators and tenants who deploy, manage, configure Cisco MSX SD-WAN service pack, and troubleshoot various SD-WAN service issues.

What's New in Cisco MSX 4.1 for SD-WAN Services

Table 1: What's New in Cisco MSX 4.1 for Cisco SD-WAN and Meraki SD-WAN Services

Feature	Description
Email Address Support in SD-WAN Orchestration Settings	A new email field is added to the SD-WAN Orchestration Settings that notifies the user about the progress in the SD-WAN processes. Only three email domains are accepted in this field: gmail.com, cisco.com, and external.cisco.com. For more information, see Configuring Cisco SD-WAN Orchestrator Settings.

Overview of Cisco MSX

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-Branch, Cisco MSX Cloud UTD, and Cisco MSX Managed Device).

For detailed information about Cisco MSX solution, see the Cisco Managed Services Accelerator (MSX) Solution Overview.

The Cisco SD-WAN and Meraki SD-WAN service packs are a suite of prepackaged software capabilities that fully automate the end-to-end SD-WAN service creation. With these fully validated service level packages, end customers can quickly turn on, control, and assure cloud-based WAN services that are offered by the service provider.

This section contains the following topics:

Cisco SD-WAN Service

Cisco MSX enables service providers to deploy and manage SD-WAN services for their customers. The deployment of an SD-WAN service in the context of a managed service requires deployment per customer and includes the SD-WAN management control plane (vManage, vBond and vSmart), and the corresponding data plane (vEdge and cEdge).

The Cisco SD-WAN service pack consists of:

- **vManage**— Cisco's GUI based centralized management and provisioning platform for Day 0, Day 1 and Day n+ for the entire Cisco SD-WAN infrastructure. You can login to the Cisco vManage dashboard to centrally manage the WAN. Cisco vManage provides the ability to manage all aspects of the WAN from provisioning, monitoring, and upgrading routers to application visibility and troubleshooting the WAN.
- **vBond**—The vBond facilitates the initial bring-up by performing initial authentication and authorization of all elements into the network. vBond provides the information on how each of the components connects to other components. It plays an important role in enabling devices that sit behind the NAT to communicate with the network.

- **vSmart Controller**—The vSmart controllers establish the secure SSL connections to all other components in the network, and run an Overlay Management Protocol (OMP) to exchange routing, security, and policy information. The centralized policy engine in vSmart provides policy constructs to manipulate routing information, access control, segmentation, extranets, and service chaining.
- **vEdge and cEdge (IOS XE) Routers**—These routers (physical and cloud) establishes secure connectivity to all of the control components and also establishes IPSec sessions with other routers in the WAN network. These routers can be used as a Virtual Network Function (VNF) deployment at the branch. NFV Infrastructure Software (NFVIS) platform on Cisco Enterprise Network Compute System (ENCS) facilitates the deployment and operation of VNFs and hardware components.

Some of the advantages of the Cisco MSX SD-WAN service pack are:

- User interface portal for ordering service (Control Plane and Data Plane Connectivity) and network visualization.
- Lifecycle management of services.
- Site and device activation.
- Site level monitoring and tunnel health reporting.
- Traffic policy management.

The table below lists supported versions of Cisco SD-WAN on Cisco MSX :

Table 2: Cisco SD-WAN and MSX Version Compatibility Matrix

Cisco MSX Release	Cisco SD-WAN Release
4.1	20.5.1 and earlier releases
4.0	20.5.1 and earlier releases
3.10	20.4.1 and earlier releases.
3.9.0	20.1.1 and earlier releases
3.8.0	19.3.0 and earlier releases
3.7.0	19.2.0 and earlier releases
3.6.0	19.1.0 and earlier releases
3.5.1/3.5.2	18.4.0 and earlier releases
3.5.0	18.3.0 and earlier releases

Cisco Meraki SD-WAN Service

All Cisco Meraki security appliances comes with SD-WAN capabilities that allow administrators to dynamically adjust to changing WAN conditions without the need for manual intervention. By providing granular control over how certain traffic types respond to changes in WAN availability and performance, SD-WAN can ensure optimal performance for critical applications and help to avoid disruptions of highly performance-sensitive traffic, such as VoIP

Using Meraki SD-WAN on MSX, service providers can add or remove networks (equivalent to adding sites in Cisco SD-WAN) and display uplink information about a device.

Some of the advantages of using Cisco Meraki SD-WAN on MSX are:

- User interface portal for ordering Meraki SD-WAN service for tenant.
- Ability to attach to a Meraki organization established for the Tenant.
- Lifecycle management of services.
- Control Plane and Data Plane Connectivity and network visualization.
- Site and device activation by selecting and applying configurations on Meraki networks.
- Site level monitoring with uplink interface details.
- Traffic policy management

The following are the Meraki wireless and combined device types currently supported on Cisco MSX:

- SD-WAN appliance devices:
  - MX64, MX65, MX67, and MX68 required for a small branch setup.
  - MX84 and MX100 required for a medium branch setup.
  - MX250 and MX450 required for a large branch/campus setup.
- vMX device types for virtual devices.
- MR device types for wireless
- MS series of access switches

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 4.1 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.

Document	Description
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.

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

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.

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.