Cisco Managed Service Accelerator (MSX) 4.3 Solution Overview Guide

First Published: 2022-05-20

CONTENTS

CHAPTER 1

Introduction

This chapter contains the following topics:

Solution Overview

Cisco MSX is a service creation and delivery platform that enables fast deployment of cloud-based and on-premise networking services for customers. Operators can deliver customizable network services using a subscription-based and pay-as-you-go model from a solution which allows them to rapidly and profitably deliver service offerings to market.

Cisco MSX also integrates with existing customer premise equipment, allowing operators to build upon and utilize the existing infrastructure. Cisco MSX provides a complete self-service user experience that allows operators and end-users to select, create, customize, and activate services on-demand in minutes from a simple, intuitive portal.

The Cisco MSX solution shifts the deployment of managed services away from the manual configuration of the latest network devices to the creation of an abstracted model representing the service definition. This approach allows the service intent of the user to be realized by using service models to automate the creation and customization of network services. Depending on the capabilities of the domain being configured, these services are instantiated either through Cisco MSX embedded Cisco Network Services Orchestrator (NSO) instance or a domain specific controller.

Through the combination of the Cisco MSX platform and service packs, the Cisco MSX solution offers a complete platform that enables Operators to offer next-generation network services.

The following are some key highlights of the Cisco MSX solution:

- Automated end-to-end, cloud-based, and on-premise services managed from public or private clouds.

- Secure multi-tenant cloud managed platform, simplified orchestration, and tenant self-service.

- Auto onboarding of devices with Zero Touch Provisioning.

- Rapidly create new monetizable services, and modify existing services instantly from the cloud.

- Perfect solution for distributed customers looking for lower cost and self-managed services.

- Open multi-vendor services catalog.

- Supports Cisco and third-party physical devices and Virtual Network Functions (VNFs).

- Develop your own service or adapt existing services.

- Can be integrated with existing OSS and BSS systems.

The chapter has the following section:

Cisco MSX Platform

Cisco MSX is a service creation platform, implementing the different functions that are required to instantiate and provision virtual and physical elements in order to construct end-to-end managed services for Service Provider and Enterprise customers. The Cisco MSX solution uses Software-Defined Networking (SDN), Network Functions Virtualization (NFV), Open APIs, and advanced orchestration capabilities to deliver a suite of business services from the cloud (public or private), over existing network infrastructure.

The Cisco MSX platform is comprised of layers,each of which abstract the layer below it and scaled horizontally. A layered abstraction approach, with well documented API contracts between the layers, allows for modularization, a key tenet of the Cisco MSX platform. The modularization allows for the separation of concerns, independent scaling, development velocity, and ultimately component replacement, if necessary.

Microservices

The Service Interface Function (SIF) and integrations are enabled as microservices that contain the logic to consume the functionality exposed by the platform. There is a standard set of microservices that expose the core platform functionality that is required to operate the platform.

Each use case can also provide one or more microservices for any use-case-specific functionality that needs to be enabled.

The following primary core microservices exist in Cisco MSX platform:

- Identity Management (IDM)—Provides user management capabilities, tenant management (tenant and tenant group), manages identity providers, user roles, permissions, secrets, password policies, and so on. Upon login, fetches the user profile and stores it in the common cache so other microservices can use it. Also provides SAML 2.0 and OAuth 2.0 capabilities for Single Sign On (SSO), authentication, and authorization capabilities.

- Catalog—Provides the capability to create services, service offers, price plans, define terms and conditions of a service, submit an order, and upgrade or downgrade a service.

- Manage—Provides the service management capabilities, such as managing customer subscriptions and device data.

- Monitor—Communicates with the service assurance components for device and service status and displays the statistics on the Portal.

- Orchestration—Communicates with NSO to process the request to create or upgrade a service chain, add or delete a device, register device serial numbers, and advanced device configurations.

- Notification—Cisco MSX provides support to trigger notifications when certain events occur. Both REST and email notifications are supported for all the events.

- Administration—Manages global activities and settings. Activities include importing bulk device settings, obtaining component versions, scheduling tasks, managing provider contacts, and user interface themes.

- Process Automation—Provides the capability to manage and execute service-oriented workflows

- Billing—Provides the capability to collect and expose billing related events.

- Incident—Enables you to integrate the Cisco MSX platform with an incident tracking system specially ServiceNow. Using this API, you can create, update, cancel, close, and delete an incident using the access token.

- Service Configuration—Manages configuration templates, track the assignment and application of those templates to a tenant.

Figure 1: Cisco MSX Infrastructure and Microservice Architecture
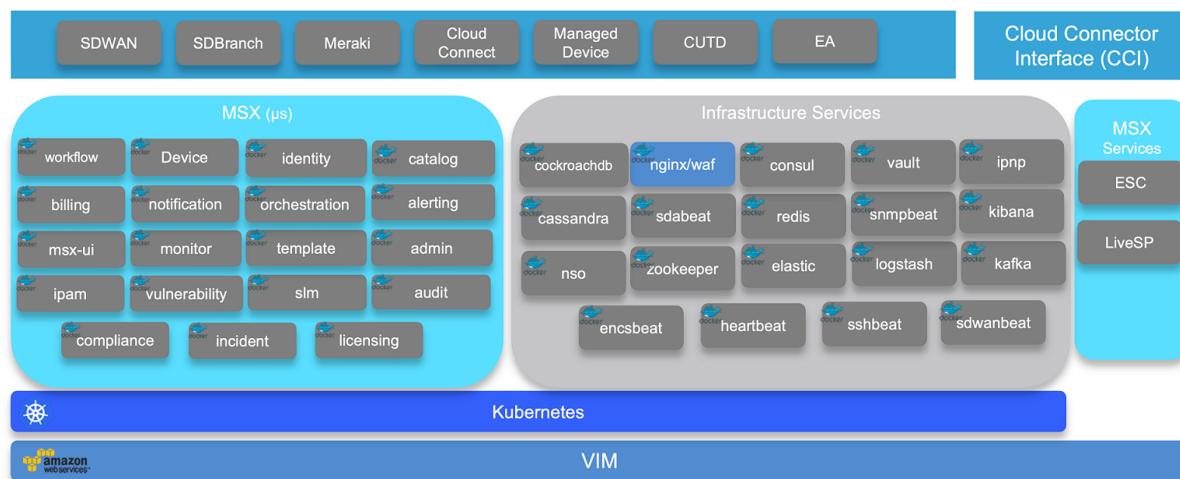
Data Platform

The data platform interface is the mechanism by which the data platform component interacts with the other platform components and applications. The major function that is performed by the data platform component is the collection of data from the platform, service packs, controllers, and devices. The collection interface provides a platform component or application the ability to instruct the data platform which data to collect, the frequency with which to collect, and how to store and correlate the data. This is to enable other platform components or external systems to augment the collection that is enabled by provisioning. For example, the instantiation of a typical service chain programs the devices participating in the chain to send data (e.g. Syslog/SNMP) to the data platform.

There are several actions that must be supported by the data platform component, and thus exposed via the service interface. The actions include, but are not limited to:

- Data Retrieval (Pull)

- Configurable Collection

- Data Subscription/Streaming (Triggers/Events)

The data platform component of the architecture is broken down into the following major sub-functions, as shown in the following illustration.

Figure 2: Data Platform Architecture Based on ELK Stack
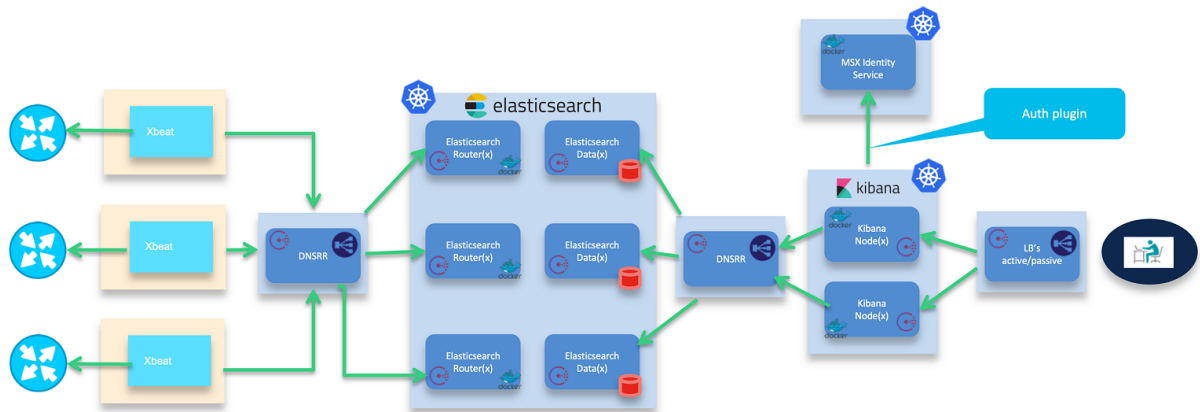
Terminology

The following table provides an alphabetical listing of Cisco MSX acronyms.

Table 1: Terminology

Acronym	Definition
AAA	Authentication, Authorization, and Accounting
ACL	Access List
API	Application Programmable Interface
ARPU	Average Revenue Per User
ASAv	Adaptive Security Appliance - vFW VNF
BGP	Border Gateway Protocol
BSS	Business Support System
CDB	Configuration Database
CFS	Consumer Facing Service
CLI	Configuration Line Interface
CMSP	Cisco Cloud and Managed Service Program
CPE	Customer Premise Equipment (ISR-G2)
CRUD	Create, Read, Update, and Delete orchestration operations
CSR	Cloud Service Router - vRouter VNF
cURL	Client URL
DC	Data Center
DCI	Data Center Interconnect

Acronym	Definition
DEST	Destination IP Address
DHCP	Dynamic Host Configuration Protocol
DMVPN	Dynamic Multi-Point Virtual Private Network
DMZ	Demilitarized Zone (Networking private to public)
DNS	Domain Name System
DST	Destination IP Address
EIGRP	Enhanced Interior Gateway Routing Protocol
ESC	Elastic Services Controller
ETS	European Telecommunications Standards
ETSI	European Telecommunications Standards Institute
EzVPN	Easy Virtual Private Network
FW	Firewall
GraphDB	Graph Data Base
GuestOS	Guest Operating System
HA	High Availability is
HDR	Header
HTTP	Hypertext Transfer Protocol
I2RS	Interface to Routing System (diagram format)
IKEv2	Internet Key Exchange version 2
IO	Input/Output
Intrusion Detection	Generally refers to the process of passively analyzing network traffic for potential intrusions and storing attack data for security analysis.
Intrusion Prevention	Includes the concept of intrusion detection, but adds the ability to block or alter malicious traffic as it travels across your network
iOS	Cisco Operating System
IP	Internet Protocol
IPSec	Internet Protocol Secure
ISR	Integrated Service Router
IT	Information Technology
KVM	Kernel-based Virtual Machine
LAN	Local Area Network
ML2	Modular Layer 2
MPLS	Multiprotocol Label Switching

Acronym	Definition
MSX	Managed Services Accelerator
NAT	Network Address Translation
NAT44	Network Address Translation IPv4-to-IPv4
NED	Network Element Driver
NEDs	Network Element Drivers
NETCONF	Network Configuration protocol
NFV	Network Functions Virtualization
NH	Next Hope
NIC	Network Interface Card
NICs	Network Interface Cards
NSO	Network Service Orchestrator
ODL	Open Daylight
OS	Operating System
OSPF	Open Shortest Path First
OSS	Operations Support System
OVS	Open Virtual Switch
PE	Provider Edge
PnP	Plug-N-Play
QEMU	Quick Emulator
QoS	Quality of Service
RA	Remote Access
REST	Representation State Transfer
RFC	Request For Comments
RFS	Resource Facing Service
ROI	Return on Investment
SA	Source Address
SDN	Solution uses software-defined networking
SLA	Service Level Agreement
SMB	Small Medium Business
SNMP	Simple Network Management Protocol
SP	Service Provider
SRC	Source IP Address

Acronym	Definition
SSH	Secure Shell
SSL	Secure Sockets layer
SUDI	Secure Unique Device Identifier
TCO	Total Cost of Ownership
TP	Termination Point
UCS	Unified Computing System
vFW	Virtual Firewall
VIM	Virtual Interface Manager
VirtIO	Virtual Input/Output
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMs	Virtual Machines
VNF	Virtual Network Function
VNFs	Virtual Network Functions
VNIC	Virtual Network Interface
VPN	Virtual Private Network
VPP	Vector Packet Parsing
VR	Virtual Router
VRF	Virtual Route Forwarding
VRRP	Virtual Registry Registrar Protocol
WAN	Wide Area Network
WCCPv2	Web Cache Communications Protocol
WSA	Web Security Appliance
WSAv	Web Security Appliance virtualized
XML	eXtensible Marking Language
YANG	Yet Another Next Generation (data modeling)
ZTD	Zero Touch Deployment

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 *Cisco MSX SD-WAN Service Pack* 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.
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)

Solution Architecture

This chapter contains the following topics:

Solution Architecture

This chapter provides insight into how the orchestration engine processes a service request, using service definition models to create and instantiate services.

This chapter contains the following sections:

Modular Architecture

As Cisco MSX evolves, the architecture continues to modularize components creating clear demarcation points between various layers in the solution, allowing maximum flexibility in both commercial and deployment models.

Cisco MSX Modules

• *Service Interface (SI)—Customer Facing Level*

The Service Interface consists of two modules, a customer facing Front-End and service request processing Back-End.

The SI Front-End is the Self-Service User Interface; from here the end-customer can select the service offer which meets their requirements. At that point, the end-customer can construct Cisco MSX services consistent with the service offer.

The SI Back-End is separate module that constructs the service request based on the end-customer choices in the Front-End module.

• *Cisco MSX Platform—Resource Facing Level*

In cases where Cisco MSX is the device configuration controller, Network Service Orchestrator provisions services based on Service Packs that logically mirror Customer Facing Service (CFS) level packages. Service packs are internal software modules that house the service models execution logic that define specific Service Packages.

In cases where Cisco MSX interacts with a device controller, Cisco MSX will leverage the API(s) provided by that controller to instantiate the appropriate outcome requested by the end-customers service request.

Cisco Network Services Orchestrator

Cisco Network Services Orchestrator (NSO) is a model-driven orchestrator which uses YANG for modeling services, and can use various methods such as NETCONF, SSH, and REST-based APIs to provision the devices. NSO receives a service intent request through the open API interface presented northbound to Cisco MSX.

Network Element Driver (NED) software modules are used to abstract out the different physical and virtual network devices to which service configuration data may be pushed. NEDs allow the same service definition models to apply to equipment from multiple vendors.

NSO runs as a container in the Cisco MSX solution. The NSO container is deployed in one of the Kubernetes nodes and monitored by the Kubernetes control plane. Service packs which utilize NSO have their own NSO container.

Cisco NSO as the Plug-and-Play Server

The Plug-and-Play (PnP) Server software element is used to handle and achieve zero-touch deployment (ZTD) for CPEs coming online and wanting to utilize the services configured through Cisco MSX. In the Cisco MSX solution, NSO also functions as the PnP server. Once a CPE device is connected to the Internet, a "call home" protocol communicates with the Cisco MSX PnP Proxy Agent. The Proxy agent is responsible for finding any NSO complexes that have registered to serve that device. Since we can only have a device registered to one NSO, if one is found, the request is forwarded to NSO. If no, NSO has registered for the device, that device is sent a BACKOFF message to try and connect again at a future time. The CPE device is fully configured using a four-step process:

- Day-(-1)—Initial config of CPE to find the PnP Server

> ✎
>
> **Note**　A new device shipped from Cisco has no knowledge of where or how to contact its PnP server. The device first reaches out to http://software.cisco.com to receive the day-(-1) configuration. After the initial configuration, a PnP redirect provides the PnP server configuration hosted by the operator.

- Day-0—Configuration of the device management interface
- Day-1—Basic interface and system configuration
- Day-2—Service-specific configuration

Inclusion of the PnP service in the Cisco MSX solution removes costly truck-rolls, which are traditionally required to install and configure each CPE device, from the service deployment. The removal of this activity greatly reduces the cost-of-service deployment, a cost that has traditionally been a pain point for Operators.

Virtual Infrastructure Manager

The Cisco MSX platform leverages or Amazon Web Services as the Virtual Infrastructure Manager (VIM) for its deployment. Cisco MSX is constructed as a collection of Docker containers that are deployed and managed using a Kubernetes cluster. This approach is used to define an open platform which facilitates automated deployment, provides scaling, and simplifies operation of containers. Cisco MSX uses Ansible to deploy and manage the construction of the basic infrastructure followed by deployment of the platform and service pack software.

Service Interface

The Cisco MSX service interface captures the service intent of the customer and realizes this intent by interacting with NSO or other domain specific controllers. The service interface is composed of two subsystems: the web portal (front-end) and the back-end.

The web portal is designed as an all-in-one web-based solution GUI. Based on the user login type, the user will be presented with one of three service interfaces: administer, operator, or user. Upon successful authentication, the user is directed to the appropriate web interface, based on the predefined role of the user.

The service interface, based on the user's role, will allow administrators to provision a tenant space for end users, while the operators can view the status of all services running, and lastly the user role is for the end-consumer to order the service based on their requirements.

From Cisco MSX 3.10 release onwards, the Cisco MSX portal displays new GUI.

The Cisco MSX GUI has:

- **The Operator Workspace:** Only visible to operator users. It lists all tenants that the operator is managing and the services they have subscribed to.

 Click on a tenant's tile to see details specific to a tenant in the Tenant Workspace GUI.

- **A Tenant Workspace:** Allows tenants to access the information related to their subscribed services.

  The menus that are available in the Tenant Workspace are:

  - **Services**: Display all services subscribed by a tenant, service status, and other service metrics.

  - **Sites**: Display an overview of the tenant's sites, site status, and allows access to site details.

  - **Devices**: Display an overview of the tenant's devices, device status, and allows access to device details.

  - **Service Controls**: Display the custom service controls that are used to manage the services.

  - **Offer Catalog**: Display existing subscriptions and allows subscribing to new services.

  - **Billing**: Display billing information about the tenant's subscriptions.

  - **Activity Feed**: The Cisco MSX portal allows a tenant to view several events pertaining to the subscriptions, sites, devices, templates, and services. The events that are logged in the **Events Log** window are also used in the Activity Feed. To view the Activity Feed, choose **Tenant Workspace > Services**. These contextual event feeds are also displayed on the **Sites Overview** window and **Devices Overview** window.

  - For more information on monitoring service status, see the Cisco Managed Services Accelerator (MSX) 4.3 Administration Documentation.

The figure below shows the Tenant Workspace:

Figure 3: Tenant Workspace
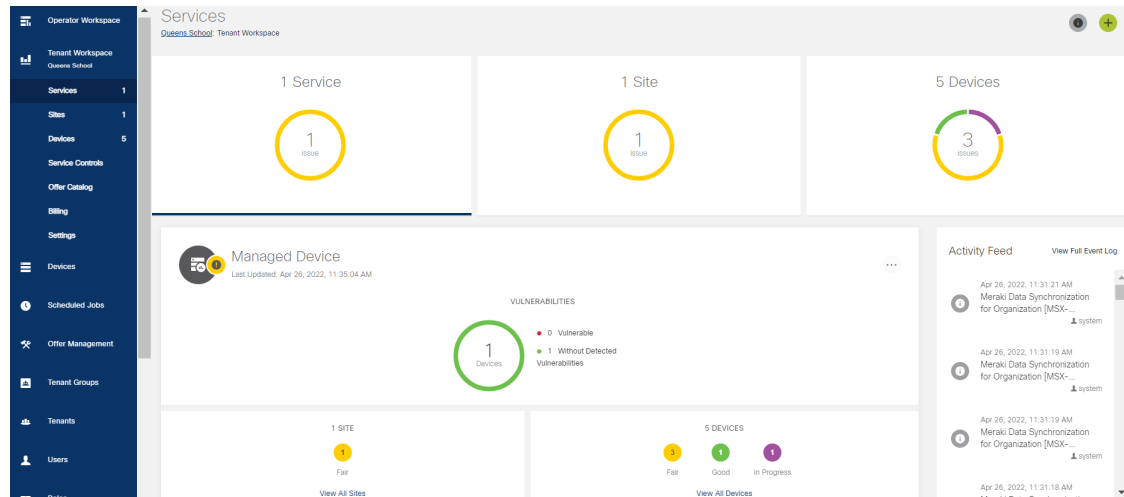
The back-end is the composition of micro-services that together communicate with various components in the Cisco MSX solution. The back-end processes the service request input using the web interface or self-service portal, and creates parametrized service requests to NSO or domain controllers.

The Cisco MSX services that are available through the portals are dependent on the service packs made available by the operator.

The service interface back-end communicates with the web portal through a REST-based API gateway. The pages of the web portal rely on back-end micro-services to process user data entered in the various portal screens. Depending on the type of data entered, the information will be sent to/from the back-end API and delivered to/sent from the micro-service responsible for processing the incoming data. The back-end micro-services are responsible for multiple functions as described in Chapter 2.

Service Packs

This chapter contains the following topics:

Service Packs

A central theme behind the Cisco MSX solution is reducing the operational cost of deploying and maintaining managed services. The solution shifts the deployment of managed services away from the manual configuration of the latest network devices to the creation of an abstracted model representing the service definition. This approach allows the service intent of the user to be realized by using the service models to automate the creation and customization of network services.

The keys to the Cisco MSX solution are virtualization, plug-n-play CPE devices, and a flexible orchestration engine capable of centralizing the configurations of all the devices involved in the delivery of a service. With flexibility inherent in the orchestration engine, operators can offer end customers the ability to order the service that best meets their technical and TCO requirements.

The Cisco MSX solution enables new services by the installation of service packs. Cisco MSX service packs can be developed by Cisco or third parties, which are then installed on top of the Cisco MSX platform and offered to end users using the Cisco MSX offer catalog.

This chapter contains the following sections:

Cisco MSX SD-WAN Service Pack

The Cisco MSX SD-WAN service pack enables operators 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 devices).

The Cisco MSX SD-WAN service pack allows the creation of a Cisco SD-WAN control plane. It also allows for seamless integration to a specific tenant's Meraki service, providing the capability to create Meraki networks and managing the devices in them.

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

• Provides the interface to associate the tenant (customer) with the Control Plane and Data Plane.

- User interface portal for ordering service (Control Plane and Data Plane Connectivity) and network visualization.

- Lifecycle management of services.

For more information on the SD-WAN service pack, see the Cisco Managed Services Accelerator (MSX) 4.3 SD-WAN Service Pack Documentation.

Cisco MSX Managed Device Service Pack

Cisco MSX Managed Device service pack enables operators to provide their customers templatized device configuration services through a self-service portal. With the Cisco MSX Managed Device service pack, IT organizations can on-board devices that are located at the customer premises (CPEs) and apply or manage configuration settings remotely from its Network Operations Center (NOC). The operator can configure parameterized configuration templates that needs to be deployed on these CPEs.

The Managed Device service pack natively supports Cisco and Meraki devices, and by loading additional NSO Network Element Drivers (NEDs) into Cisco MSX, support can be extended to devices from over a hundred third party vendors. The Cisco MSX Managed Devices service pack supports device compliance and detects changes in device configuration made by remote users. The Cisco MSX Managed Devices service pack facilitates Meraki device management, allowing operators to manage organizations and build networks using Meraki devices and services. The Cisco MSX Managed Device service pack makes device deployment fast and easy. Some of the advantages are as follows:

- Zero touch provisioning for initial device connectivity through PnP server processes.

- Service provisioning of on-premises routers through NSO orchestration.

- User Interface portal for configuration templates, ordering service, and performance or fault monitoring.

For more information on the Managed Device service pack, see the Cisco Managed Services Accelerator (MSX) 4.3 Managed Device Service Pack Documentation.

Cisco MSX Enterprise Access Service Pack

The Cisco MSX Enterprise Access provides consistent management and automation of an Enterprise Network Fabric (wired and wireless network infrastructure). Cisco MSX Enterprise Access DNA-Controller allows operators to offer managed intent-based policy and network segmentation as well as traditional LAN/WAN provisioning from one central place. Cisco MSX Enterprise Access also provides the network health at the global enterprise level by transparently aggregating all the enterprise network domains in a single pane of glass.

Benefits of using Cisco MSX Enterprise Access:

- Enables enterprise customers to monitor the health of their network.

- Gives network architects the tools to orchestrate key business functions like onboarding, secure segmentation, IoT integration, and guest access.

- Enables policy-based automation from the edge to the cloud.

- Automates user and device policy for any application across the wireless and wired network via a single network fabric.

- Federated Management of multiple Cisco DNA Center controllers per Cisco MSX Tenant.

- Configuration and provisioning for external network services access (Fusion Router Configuration for Enterprise Access).

- Cisco DNA Center and end-point bulk updates.

- Centralized template management.

- WLAN Provisioning for Non-Fabric deployment.

- Automated Configuration of Cisco DNA Center Appliances.

For more information on the Enterprise Access service pack, see the Cisco Managed Services Accelerator (MSX) 4.3 Enterprise Access Service Pack Documentation.