Intersight Device Connector

This chapter describes how to connect devices in a secure way to send information and receive control instructions on Cisco MDS 9000 Family switches.

Device Connector

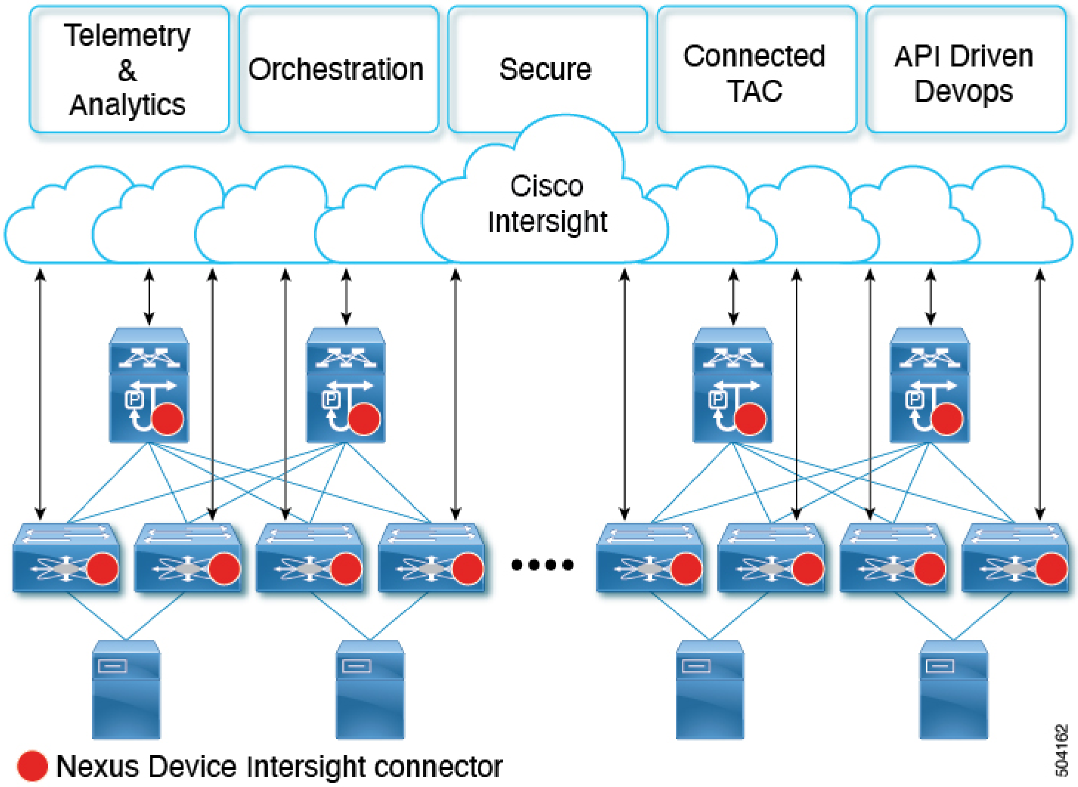
Beginning with Cisco NX-OS MDS 9000 Release 9.3(2), the Device Connector on NX-OS feature is supported which provides a secure way for the connected devices to send information and receive control instructions from the Cisco Intersight portal, using a secure Internet connection.

The Cisco MDS 9000 switch must properly resolve svc.intersight.com and allow outbound initiated HTTPS connections on port 443. To resolve svc.intersight.com, you must configure DNS on the Cisco MDS 9000 devices. If a proxy is required for an HTTPS connection to svc.intersight.com, the proxy can be configured in the NXDC user interface. .

The NXDC is enabled by default on all Cisco MDS 9000 series switches and it starts at boot by default, and attempts to connect to the cloud service. Once a secure connection has been established and the device connector is registered with the Intersight service, the device connector collects detailed inventory, health status and sends the adoption telemetry data to the Intersight database. Inventory is refreshed once in a day.

The NXDC feature integration resolves not managed switches with the following capabilities:

- It provides fast and quick solution to gather basic data from unmanaged switches.
- It stores private and organized data of all devices in a single location.
- It manages the data securely in the cloud.
- It is flexible for future extensions and upgradability.



Guidelines and Limitations for Device Connector

The following are the guidelines and limitations for Device Connector.

- Extra port may be displayed during a port scan. The ports are seen only in the local IPv4 or IPv6.

Configuring NXDC

To configure NXDC, follow the below steps:

Note By default the NXDC feature is enabled.

SUMMARY STEPS

1. **no feature intersight**
2. **intersight proxy** <*proxy-name*> **port** <*proxy-port*>
3. **intersight connection** <*name*>
4. **intersight trustpoint** <*trustpoint-label*>

DETAILED STEPS

	Command or Action	Purpose
Step 1	**no feature intersight** **Example:** `switch(config)# no feature intersight`	Disables the intersight process and removes all NXDC configuration and logs store.
Step 2	**intersight proxy** <*proxy-name*> **port** <*proxy-port*> **Example:** `switch(config)# intersight proxy proxy.esl.cisco.com port 8080`	Configures the proxy server for intersight connection. • *proxy-name*: IPv4 or IPv6 address or DNS name of proxy server. • *proxy-port*: Proxy port number. The range is 1-65535. The default value is 8080. **Note** If Proxy is enabled with the smart license configuration on Cisco MDS 9000 switches, the NXDC inherits this configuration and attempts to connect with Cisco Intersight Cloud.
Step 3	**intersight connection** <*name*> **Example:** `switch(config)# intersight connection qaconnect.starshipcloud.com`	Sets the DNS name for intersight connection. It can be used to change from intersight to NDSaaS. • *name*: Name value is string. The maximum size is 128.
Step 4	**intersight trustpoint** <*trustpoint-label*> **Example:** `switch(config)#intersight trustpoint mds-stage-onprem`	Configures certificates for intersight connection. *trustpoint-label*: Crypto ca truspoint label. For more information refer to *Cisco MDS 9000 Series NX-OS Security Configuration Guide*.

Verifying NXDC

To verify the NXDC configuration, use the following commands:

Command	Purpose
show system internal intersight info	Displays the device connector system info. switch(config)# **show system internal** **intersight info** Intersight connector.db Info: AccountOwnershipState :Not Claimed AccountOwnershipUser : AccountOwnershipTime :0001-01-01T00:00:00Z AccountOwnershipId : DomainGroupMoid :5b2541877a7662743465ccad AccountMoid :5960901ca94eba000127e335 CloudDns :svc.ucs-connect.com CloudDnsList: 1. :svc-static1.ucs-connect.com 2. :svc.ucs-connect.com 3. :svc.intersight.com 4. :svc-static1.intersight.com Identity :63931a496f72612d3922c706 CloudEnabled :true ReadOnlyMode :false LocalConfigLockout :false TunneledKVM :false HttpProxy: ProxyHost :proxy-wsa.esl.cisco.com ProxyPort :80 Preferenc :0 ProxyType :Manual Target[1]: ProxyHost :proxy-wsa.esl.cisco.com ProxyPort :80 Preference :0 LogLevel :info DbVersion :1 AutoUpgradeAdminState :Automatic
show system internal intersight connection state	Displays the device connections. switch(config)# **show system internal** **intersight connection-state** AdminState : true ReadOnlyMode : false ConnectionState : Connected ConnectionStateQualifier : ConnectionLastDownTimeTs : 2022-12-09T11:21:33.653652476Z AccountOwnershipState : Not Claimed AccountOwnershipUser : AccountOwnershipTime : 0001-01-01T00:00:00Z AccountOwnershipName : Leadership : Primary DeviceRegistrationMoid : 63931a496f72612d3922c706

The following adoption telemetry data is collected from switch and sent to Intersight.

Type	Data
Inventory	Device Name
	Product Type
	Version
	Serial number
	Cpu average load
	Memory usage
	Disk name, usage
	Device Up Time
	Device Id
	Interface information – name , up count, down count, operational state, transceiver status
	Telnet enable status
	Bootflash model, serial number
	Last Reboot Time
	Last Reset Reason
	System Up Time
License details	List of activated licenses
Feature details	List of activated features
Power Supply details	Product Id
	Serial Number
	Vendor Id
Fan details	Product Id
	Serial Number
	Vendor Id
Module details	Product Id
	Serial Number
	Vendor Id
Transceiver Details	Product Id
	Serial Number
	Vendor Id
	Part Number
Neighbor details	WWN of the neighbor switches in the fabric