Oracle Communications IP Service Activator™ Cartridge
Version 5.2.4

Cisco IOS Cartridge Guide

Second Edition
December 2008

Copyright and Trademark Information

Contents

About this Guide

The Cisco IOS Cartridge Guide provides detailed technical information about IP Service Activator features, device configuration information, and sample device configuration for Cisco IOS devices.

Audience

This guide is intended for network managers and technical consultants responsible for implementing IP Service Activator within a network using Cisco devices.

Before contacting Oracle Global Customer Support (GCS)

If you have an issue or question, Oracle recommends reviewing the product documentation and articles on MetaLink in the Top Technical Documents section to see if you can find a solution. MetaLink is located at http://metalink.oracle.com.

In addition to MetaLink, product documentation can also be found on the product CDs and in the product set on Oracle E-Delivery.

Within the product documentation, the following publications may contain problem resolutions, work-arounds and troubleshooting information:

- Release Notes
- Oracle Installation and User's Guide
- README files

Contacting Oracle Global Customer Support (GCS)

You can submit, update, and review service requests (SRs) of all severities on MetaLink, which is available 24 hours a day, 7 days a week. For technical issues of an urgent nature, you may call Oracle Global Customer Support (GCS) directly.

Oracle prefers that you use MetaLink to log your SR electronically, but if you need to contact GCS by telephone regarding a new SR, a support engineer will take down the information about your technical issue and then assign the SR to a technical engineer. A technical support representative for the Oracle and/or former MetaSolv products will then contact you.

Note that logging a new SR in a language other than English is only supported during your local country business hours. Outside of your local country business hours, technical issues are supported in English only. All SRs not logged in English outside of your local country business hours will be received the next business day. In order to obtain the broadest access to skilled technical support, Oracle advises you to log new SRs in English.

Oracle GCS can be reached locally in each country. Refer to the Oracle website for the support contact information in your country. The Oracle support website is located at http://www.oracle.com/support/contact.html.

Downloading products and documentation

To download the Oracle and/or former MetaSolv products and documentation, go to the Oracle E-Delivery site, located at http://edelivery.oracle.com.

You can purchase a hard copy of Oracle product documentation on the Oracle store site, located at http://oraclestore.oracle.com.

For a complete selection of Oracle documentation, go to the Oracle documentation site, located at http://www.oracle.com/technology/documentation.

Downloading a media pack

To download a media pack from Oracle E-Delivery

1. Go to http://edelivery.oracle.com.
2. Select the appropriate language and click **Continue**.
3. Enter the appropriate **Export Validation** information, accept the license agreements and click **Continue**.
4. For **Product Pack**, select **Oracle Communications Applications**.
5. For **Platform**, select the appropriate platform for your installation.
6. Click **Go**.
7. Select the appropriate media pack and click **Continue**.
8. Click **Download** for the items you wish to download.
9. Follow the installation documentation for each component you wish to install.

IP Service Activator publications

The IP Service Activator documentation suite includes a full range of publications. Refer to the IP Service Activator *Release Notes* for more information.

Cartridge Overview

The IP Service Activator cartridges enable you to quickly, cost-effectively, and seamlessly support your existing services, and also continuously evolve to support emerging services and business needs. The cartridges operate in conjunction with IP Service Activator core product. These cartridges offer the following benefits:

Reduced Time to Market—time to market of new services is reduced through simplified development, implementation, and extension of cartridges on customer sites.

Extendable—cartridges can be extended to include additional services and components that deliver business value, without requiring changes to the original cartridge.

Simplified Effort—the effort and technical knowledge that is required to perform customizations is reduced.

Ease of Installation—cartridges can be installed without interfering with the existing IP Service Activator install base.

Features

This chapter outlines IP Service Activator support for Cisco devices. The IP Service Activator supported features are listed in the following tables.

Legend

Feature support is indicated in each table, according to the following legend:

Icon	Definition
●	Supported
◖	Partially supported
○	Not supported

General IP Service Activator features

IP Service Activator Feature	Cisco IOS Cartridge
Configuration Protocol Support	
Telnet	●
SSH	●
SNMP	○
Vendor Proprietary	○
Device Discovery	
SNMP	●
Discovery Module	○
Device Configuration	
Configuration Audit	●
Command Re-issue	●
Auto ID Migration	●
Save Running Configuration	●
Configuration Version	●
Configuration Options	●
Synonyms	●
Command Thresholding	●
Threshold Activated Configuration Control	●
Supported Services	
Interface Configuration Management	●
QoS	●
Layer 3 MPLS VPN	●
Point-to-Point CCC	○
Point-to-Point VLL Martini	○
VPLS	○
SAA	●
Netflow	●
Dynamic User VPN	○
IPSec	○
VRF-aware IPSec	●
LSP	○

VLAN	●
Base Configuration Policies	●
Layer 2 QoS	●
Qos Attachment	●
VRF Route Maps	●
VPN and IP Multicast Module	●
Configuration Template Manager	●
SDK	
Service Cartridge SDK	●
Configuration Policy SDK	●

Layer 3 MPLS VPN

IP Service Activator Feature	Cisco IOS Cartridge
Layer 3 MPLS VPN Support	●
Topology	
Mesh	●
Hub and spoke	●
Management	●
Addressing	
Public IP	●
Private IP	●
Unnumbered	●
Interface description	●
VRF Table	
VRF export map reference	●
VRF import map reference	●
VRF DHCP Helper	○
VRF Description	●
VRF Label	○
VRF Route Targets	●
VRF Table Name	●
VRF Route Distinguisher	●
VRF route limit (max routes)	●
EIBGP Multi-path load sharing	●
EBGP Multi-path load sharing	●
EIGRP Multi-path load sharing	○
IBGP Multi-path load sharing	●
IBGP unequal-cost	●
VRF Import (max paths)	●
VRF Target	○
VRF Reduction	●
Force install	●
Shareable	●
OSPF Router ID	●
Interface-less VRF	●
Static routing	●
Static Global routes	●
Static Local Routes (redistribution)	●
Static Permanent routes	●
Static Tag Value	●
Static next hop IP address	●
Static next hop interface	●
Static next hop IP and interface	●

IP Service Activator Feature	Cisco IOS Cartridge
Static Route to Null0	●
BGP	
BGP Network Statements	●
BGP Aggregate Statements	●
eBGP	●
EBGP AS override	●
EBGP Site of Origin	●
Remove private AS	●
EBGP Update source	●
EBGP Multihop	●
EBGP Allow AS in	●
EBGP PE-CE MD5 authentication	●
EBGP Local AS	●
EBGP Local AS No prepend	●
EBGP Neighbor Description	●
EBGP Soft Reconfiguration	○
EBGP Prefix Limit	●
EBGP Prefix Limit Restart	●
EBGP Prefix filters	●
EBGP Standard community attributes	●
EBGP Extended community attributes	●
EBGP Timers	●
Keep alive	●
Hold Timer	●
EBGP Neighbor Advertisement Interval	●
EBGP Inbound Route Map	●
External Route Map	●
Generated Route Map	●
EBGP Local preference	●
EBGP Site of Origin route-map	●
Route Map Name	●
EBGP Outbound Route Map	●
External Route Map	●
EBGP Route dampening	●
Redistribution into BGP	●
BGP Redistribution Metric and Policy from Connected	●
BGP Redistribution Metric and Policy from Static	●
BGP Redistribution Metric and Policy from RIP	●
BGP Redistribution Metric and Policy from OSPF	●
BGP Redistribution Metric and Policy from EIGRP	●
Default Route	●
OSPF	●
OSPF Area Type	●
OSPF NSSA Type 7 Redistribution	●
OSPF Maximum Paths	●
OSPF Cost	●
OSPF BGP Redistribution tag	●
OSPF Distribute in filter	●
OSPF Distribute out filter	●
OSPF SPF Throttling	●
OSPF MD5 authentication	●
OSPF Summary Addresses	●
Suppress Advertise	●

IP Service Activator Feature	Cisco IOS Cartridge
Tag Value	●
Redistribution into OSPF	●
OSPF Redistribution Metric and Policy from Connected	●
OSPF Redistribution Metric and Policy from Static	●
OSPF Redistribution Metric and Policy from RIP	●
OSPF Redistribution Metric and Policy from BGP	●
OSPF Redistribution Metric and Policy from EIGRP	●
Default Route	●
RIP	●
RIP Ignore Routes from Source	●
RIP Passive Interface	●
Redistribution into RIP	●
RIP Redistribution Metric and Policy from Connected	●
RIP Redistribution Metric and Policy from Static	●
RIP Redistribution Metric and Policy from OSPF	●
RIP Redistribution Metric and Policy from BGP	●
RIP Redistribution Metric and Policy from EIGRP	●
Default Route	○
EIGRP	●
EIGRP Device ASN	●
EIGRP Site ASN	●
EIGRP Site of Origin	●
EIGRP Route-map name for SOO	●
EIGRP MD5 Authentication	●
EIGRP Maximum Paths	●
EIGRP Redistribution	●
EIGRP Redistribution Metrics and Policy from Connected	●
EIGRP Redistribution Metrics and Policy from Static	●
EIGRP Redistribution Metrics and Policy from BGP	●
EIGRP Redistribution Metrics and Policy from OSPF	○
EIGRP Redistribution Metrics and Policy from RIP	●

Layer 2 VLL

IP Service Activator Feature	Cisco IOS Cartridge
Circuit Cross Connect	○
ATM AAL5	○
ATM Cell	○
Ethernet	○
Ethernet VLAN	○
Frame	○
HDLC	○
PPP	○
Martini Point-to-Point	
ATM AAL5	●
ATM Cell	●
Ethernet	●
Ethernet VLAN	●
Frame	●

Port Based	○
Port and VLAN Tagged	○

VLAN

IP Service Activator Feature	Cisco IOS Cartridge
VLAN (TLS L2 Site)	○
Tagged VLAN	○
Untagged VLAN	○
VLAN Module	●
Tagged VLAN	●
Untagged VLAN	●
Queue-in-Queue VLAN	●
vlanDefinitions	●
VLAN State	●
VLAN Media (Type): Ethernet	●
Maximum Transmission Unit (MTU)	●
Security Association Identifier (SAID)	●
vlanInterface	●
Tagged VLAN: Encapsulation Type	●
Encapsulation Type: dot1 q	●
Encapsulation Type: isl	●
Tagged VLAN: Switchport No negotiate	●
Tagged VLAN: Native VLAN	●
Tagged VLAN: VLAN Range	●
Untagged VLAN	●
Queue-in-Queue VLAN	●

LSP

IP Service Activator Feature	Cisco IOS Cartridge
LSP Module	●
Primary Tunnel	●
Backup Tunnel	●
Bypass Tunnel	○
Setup Priority	●
Hold Priority	●
Affinity	●
IGP Metric	●
Fast Reroute	●
Record Route	●
LDP Enabled	●

QoS

IP Service Activator Feature	Cisco IOS Cartridge
Layer 3 Qos Support	●
Access Rule Support	●
Inbound Access Rule Support	●
Outbound Access Rule Support	●
Logging	●
Suppress Management Traffic terms	●
Named ACL support	●
Numbered ACL support	●
Guarantees Supported	○
Limits Supported	○
Access Rule Classification Criteria	●
Access Rule Classification based on Source IPv4 Address	●
Access Rule Classification based on Destination IPv4 Address	●
Access Rule Classification based on Source IP Port	●
Access Rule Classification based on Destination IP Port	●
Access Rule Classification based on IP Protocol	●
Access Rule Classification based on DiffServ Codepoints	●
Access Rule Classification based on IPv4 Precedence Codepoints	●
Access Rule Classification based on IPv4 TOS Codepoints	○
Access Rule Classification based on URL	○
Access Rule Classification based on MIME Type	○
Access Rule Classification based on Application protocol	○
Access Rule Classification based on Application Type	○
Access Rule Classification based on Domain Name	○
Access Rule Classification based on 802.1p User Priority	○
Access Rule Classification based on MPLS EXP value	●
Access Rule Classification based on TCP Flag values	●
Access Rule Classification based on ICMP Flag values	●
Access Rule Classification based on Fragments	●
Traffic Classification Rules	●
Inbound Traffic Classification Rule Support	●
Outbound Traffic Classification Rule Support	●
Named ACL support	●
Traffic Classification Rule Criteria	●
Traffic Classification based on Source MAC Address	○
Traffic Classification based on Destination MAC Address	○
Traffic Classification based on Source IPv4 Address	●
Traffic Classification based on Destination IPv4 Address	●
Traffic Classification based on Source IP Port	●
Traffic Classification based on Destination IP Port	●
Traffic Classification based on IP Protocol	●
Traffic Classification based on all DiffServ Code Points	●
Traffic Classification based on IPv4 Precedence Codepoints	●
Traffic Classification based on IPv4 TOS Codepoints	○
Traffic Classification based on URL	●
Traffic Classification based on MIME Type	●
Traffic Classification based on Application protocol	●
Traffic Classification based on Application Type	○
Traffic Classification based on Domain Name	○
Traffic Classification based on 802.1p User Priority	○

Traffic Classification based on MPLS EXP value	●
Traffic Classification based on TCP Flag bits	●
Traffic Classification based on ICMP Flag values	●
Traffic Classification based on fragments	●
Traffic Classification Marking	●
Marking DiffServ Code Points	●
Marking IPv4 IP Precedence	●
Marking IPv4 TOS	○
Marking 802.1p User Priority	○
Marking: MPLS Experimental Bit	●
Marking: Topmost MPLS Experimental Bit	●
Discard Class	●
Trust Type	●
Traffic Policing Rules	●
Inbound Traffic Policing Rule Support	●
Outbound Traffic Policing Rule Support	●
Policing Rule: Named ACL support	●
Policing Rule Classification Criteria	●
Policing Classification based on Source MAC Address	○
Policing Classification based on Destination MAC Address	○
Policing Classification based on Source IPv4 address	●
Policing Classification based on Destination IPv4 Address	●
Policing Classification based on Source IP Port	●
Policing Classification based on Destination IP Port	●
Policing Classification based on IP Protocol	●
Policing Classification based on all DiffServ Code Points	●
Policing Classification based on IPv4 Precedence Codepoints	●
Policing Classification based on IPv4 TOS Codepoints	○
Policing Classification based on URL	○
Policing Classification based on MIME Type	○
Policing Classification based on Application protocol	○
Policing Classification based on Application Type	○
Policing Classification based on Domain Name	○
Policing Classification based on 802.1p User Priority	○
Policing Classification based on MPLS EXP value	●
Policing Classification based on TCP flags	●
Policing Classification based on ICMP Flag values	●
Policing Classification based on fragments	●
Policing Rule Marking Actions	●
Policing: Marking DiffServ Code Points	●
Policing: Marking IP Precedence	●
Policing: Marking IPv4 TOS	○
Policing: Marking 802.1p User Priority	○
Policing: Marking: MPLS Experimental Bit	●
Policing: Marking Topmost MPLS Experimental Bit	●
Standard PHB Group Support	●
PHB WRR	○
PHB WRR Inbound	○
PHB WRR Outbound	○
PHB Priority Queuing	○
PHB Priority Queuing Inbound	○
PHB Priority Queuing Outbound	○
PHB Weighted Fair Queuing	●
PHB WFQ Inbound	●
PHB WFQ Outbound	●
PHB-WFQ Class-based Queuing Support	●

PHB-WFQ Discard Eligibility Marking	●
PHB-WFQ PQ Percentage Bandwidth Support	●
PHB-WFQ Low Priority Queue Percentage Bandwidth Support	●
PHB-WFQ Per-queue WRED Support	●
PHB-WFQ Per-queue Tail Drop Limits	●
PHB Congestion Avoidance: WRED	●
PHB Inbound WRED	○
PHB Outbound WRED	●
PHB WRED: DSCP Support	●
PHB WRED: IPv4 Precedence	●
PHB WRED: Parameters	●
PHB WRED: Min Threshold	●
PHB WRED: Max Threshold	●
PHB WRED: Weight Factor	●
PHB WRED: Exponential Weight Constant	●
PHB: Explicit Congestion Notification	●
PHB Rate Limiting	○
PHB Inbound Rate Limiting	○
PHB Outbound Rate Limiting	○
PHB Rate Limit Average	○
PHB Rate Limit Burst Rate	○
PHB Rate Limit Burst Interval	○
PHB Frame Relay Fragmentation	●
PHB FRF.12	●
PHB Frame Relay Traffic Shaping	●
PHB FRTS – CIR	●
PHB FRTS – MINCir	●
PHB FRTS – BC	●
PHB FRTS - BE	●
PHB Inbound CIR	●
PHB Inbound MINCIR	●
PHB Inbound BC	●
PHB Inbound BE	●
PHB BECN	●
PHB FECN	●
PHB Frame Relay Hold-Queue depth	●
PHB ATM Traffic Shaping	●
PHB Outbound ATM Traffic Shaping	●
PHB Inbound ATM Traffic Shaping	○
PHB ATM Service Classes	●
PHB ATM Service Class – UBR	○
PHB ATM Service Class – CBR	●
PHB ATM Service Class - RT VBR	●
PHB ATM Service Class - NRT VBR	●
PHB ATM Service Class – ABR	○
PHB ATM Service Class - VC-Class Map Generation	●
PHB ATM Service Class - VC-Class Map Explicit Naming	●
PHB ATM Hold-Queue Depth	●
PHB ATM TX-Ring Limit Support	●
MQC-PHB Support	●
MQC-PHB Classification Criteria	●
Traffic Classification Explicit ACL Number Specification	●
Traffic Classification Explicit ACL Name Specification	●
Traffic Classification based on Source MAC Address	●
Traffic Classification based on Destination MAC Address	●
Traffic Classification based on Source IPv4 Address	●

Traffic Classification based on Source Ipv6 Address	●
Traffic Classification based on Destination IPv4 Address	●
Traffic Classification based on Destination Ipv6 Address	●
Traffic Classification based on Source IP Port	●
Traffic Classification based on Destination IP Port	●
Traffic Classification based on IP Protocol	●
Traffic Classification based on all Ipv4 DiffServ Code Points	●
Traffic Classification based on all IPv6 DiffServ Code Points	●
Traffic Classification based on URL	●
Traffic Classification based on MIME Type	●
Traffic Classification based on Application protocol	●
Traffic Classification based on MPLS EXP value	●
Traffic Classification based on ATM Cell Loss Priority	○
Traffic Classification - Nested Class Map	●
Traffic Classification Match Any Support	●
Traffic Classification Exclude Option	●
Traffic Classification based on TCP Flag Bits	●
Traffic Classification based on ICMP Flag values	●
Traffic Classification based on IP Precedence	●
Traffic Classification based on fragments	●
Traffic Classification RTP Protocol Port	●
Compound Traffic Classification	●
LLQ	●
LLQ Inbound	○
LLQ Outbound	●
LLQ Absolute Bandwidth Support	●
LLQ Percentage Bandwidth Support	●
LLQ Percentage Remaining Bandwidth Support	○
LLQ Device Default Bandwidth	●
LLQ Burst Support	●
Class Based Weighted Fair Queue CBWFQ	●
CBWFQ Inbound	○
CBWFQ Outbound	●
CBWFQ Absolute Bandwidth Support	●
CBWFQ Percentage Bandwidth Support	●
CBWFQ Remaining Percentage Bandwidth Support	●
CBWFQ Queue Limit Support	●
Fair-queue Flow queue-limit Default	●
Fair-queue Flow queue-limit Limit	●
CBFQ Max Reserved Bandwidth	●
MQC-PHB Default WFQ	●
MQC-PHB Default WFQ Inbound	○
MQC-PHB Default WFQ Outbound	●
MQC-PHB Default Reserved Bandwidth Control	●
MQC-PHB Single Rate Policing	●
MQC-PHB Single Rate Policing Inbound	●
MQC-PHB Single Rate Policing Outbound	●
MQC-PHB Single Rate Policing Absolute Rate	●
MQC-PHB Single Rate Policing Percent Rate	●
Default CBS	●
Default EBS	●
MQC-PHB Two Rate Policing	●
MQC-PHB Two Rate Policing Inbound	●
MQC-PHB Two Rate Policing Outbound	●
MQC-PHB Two Rate Policing Absolute Rate	●
MQC-PHB Two Rate Policing Percent Rate	●

MQC-PHB Policing Actions	●
MQC-PHB Policing: Drop	●
MQC-PHB Policing: Set IP Precedence	●
MQC-PHB Policing: Set DiffServ Code Points	●
MQC-PHB Policing: Set MPLS Exp	●
MQC-PHB Policing: Set FR DE	O
MQC-PHB Policing: Set ATM CLP	O
MQC-PHB Shaping Support	●
MQC-PHB Shaping: Inbound	O
MQC-PHB Shaping: Outbound	●
MQC-PHB Shaping: Default Shaping	●
MQC-PHB Shaping: Shape Average	●
MQC-PHB Shaping: Shape Peak	●
MQC-PHB Shaping: Default Bc	●
MQC-PHB Shaping: Default Be	●
MQC-PHB Maximum Number of Shaping Buffers	●
MQC-PHB: FRTS Support	●
MQC-PHB: FRTS Inbound	●
MQC-PHB: FRTS Outbound	●
MQC-PHB: FRTS MINCir	●
MQC-PHB: FRTS BECN	●
MQC-PHB: FRTS FECN	●
MQC-PHB Marking Support	●
MQC-PHB Marking Inbound	●
MQC-PHB Marking Outbound	●
MQC-PHB Marking: DiffServ Code Point Support	●
MQC-PHB Marking: MPLS Experimental Bit Support	●
MQC-PHB Marking TopMost MPLS EXP Support	●
MQC-PHB Marking Frame Relay Discard Eligibility Bit Support	O
MQC-PHB Marking ATM Cell Loss Priority Support	O
MQC-PHB Marking IP Precedence	●
MQC-PHB Marking IPv4 TOS	O
MQC-PHB Marking IPv4 Discard Class	●
MQC-PHB Marking Trust Type	●
MQC-PHB Congestion Avoidance	●
MQC-PHB Inbound congestion avoidance	O
MQC-PHB Outbound congestion avoidance	●
Tail Drop Limit	●
Tail Drop Default	●
MQC-PHB WRED Device Default Parameters	O
MQC-PHB WRED IP Precedence Support	●
MQC-PHB WRED DSCP Support	●
MQC-PHB Nesting Support	●
MQC-PHB Inbound Nesting	●
MQC-PHB Outbound Nesting	●
MQC-PHB Header Compression	●
MQC-PHB RTP Header Compression Support	●
MQC-PHB TCP Header Compression Support	O

Layer 2 QoS

IP Service Activator Feature	Cisco IOS Cartridge
catOSPolicingRule Configuration Policy	○
Policing Rule IP Classification Criteria	○
Classification based on Trust Type	○
Classification based on DiffServ Code Point	○
Classification based on Source IPv4 Address	○
Classification based on Destination IPv4 Address	○
Policing Rule MAC Classification Criteria	○
Classification based on Trust Type	○
Classification based on DiffServ Code Point	○
Classification based on Source MAC Address	○
Classification based on Destination MAC Address	○
Policing Rule IPX Classification Criteria	○
Classification based on Trust Type	○
Classification based on DiffServ Code Point	○
Classification based on Source MAC Address	○
Classification based on Destination MAC Address	○
Classification based on Protocol	○
Classification based on Source IPX Address	○
Classification based on Destination IPX Address	○
rate-limit Configuration Policy	○
qosCosAttachment Configuration Policy	●

Service Assurance

IP Service Activator Feature	Cisco IOS Cartridge
Service Assurance Probe	●
Service Assurance Probe Types	●
ICMP Echo Probe	●
UDP Jitter Probe	●
TCP Connect Probe	●
UDP Echo Probe	●
ICMP Jitter Probe	○
VoIP UDP Jitter Probe	○
RTP-based VoIP Probe	○
VoIP Gatekeeper Delay Monitoring	○
VoIP Call Setup (Post Dial Delay) Monitoring	○
HTTP Probe	○
ICMP Path Echo Probe	○
ICMP Path Jitter Probe	○
FTP Probe	○
DNS Probe	○
DHCP Probe	○
DLSw+ Probe	○
SA Probe Transmission Parameters	●
SA Probe Timeout	●
SA Probe Frequency	●
SA Probe Lifetime	●

SA Probe Request Size	●
SA Destination Port	●
SA Source Port	●
SA Probe Source IP Address	●
SA DSCP	●
SA Probe Destination IP Address	●
SA Packets in Sequence	●
SA Inter-packet Interval	●
SA Probe Reaction configuration	●
SA Reaction configuration - Supported Threshold Types	●
Immediate	●
Average	●
Consecutive	●
Never	●
X of Y	●
SA Reaction configuration - Supported Action Types	●
Trigger	●
Trap	●
SNA Nmvt	●
External System IP	●
SA Probe History	●
Lives Kept	●
Filter	●
Buckets	●
SA MD5 Support	○
SA Probe Numbering	●
SA Explicitly specified probe identifiers	○
SA Auto-generated probe identifiers	●
SA Probe Checks	●
SA Error Checking	●
SA Connect Checking	●
SA Timeout Checking	●
rtrResponder Configuration Policy	●

Netflow

IP Service Activator Feature	Cisco IOS Cartridge
Measurement Parameters	○
Collect NetFlow Statistics	○
NetFlow Cache Entries	○
NetFlow Active Timeout	○
NetFlow Inactive Timeout	○
NetFlow Aggregation	○
NetFlow Aggregation Schemes	○
NetFlow Autonomous System Aggregation Scheme	○
NetFlow Destination Prefix Aggregation Scheme	○
NetFlow Prefix Aggregation Scheme	○
NetFlow Protocol Port Aggregation Scheme	○
NetFlow Source Prefix Aggregation Scheme	○
NetFlow Aggregation Cache Entries	○
NetFlow Aggregation Active Timeout	○
NetFlow Aggregation Inactive Timeout	○
NetFlow Aggregation Export Destinations	○
NetFlow Export Version	○

NetFlow Export Source	○
NetFlow Export Destinations	○
NetFlow Ingress Accounting on Interface	○
Sampled NetFlow	○
Sampled NetFlow on Interface	○
Sampled NetFlow Packet Interval	○
Collect CAR QoS MIB Statistics	○
Collect Juniper CoS MIB Statistics	○
Collect MIB2 Statistics	○
collectorParameters Configuration Policy	●
Cisco Netflow FlowCollector	●
InfoVista Netflow	●
netflowParameters Configuration Policy	●
NetFlow Cache	●
NetFlow Active Timeout	●
NetFlow Inactive Timeout	●
NetFlow Aggregation	●
NetFlow Aggregation Schemes	●
NetFlow Autonomous System Aggregation Scheme	●
NetFlow Destination Prefix Aggregation Scheme	●
NetFlow Prefix Aggregation Scheme	●
NetFlow Protocol Port Aggregation Scheme	●
NetFlow Source Prefix Aggregation Scheme	●

VRF-aware IPSec

IP Service Activator Feature	Cisco IOS Cartridge
customerIPsec Configuration Policy	●
publicIPsec Configuration Policy	●

VRF and IP Multicast

IP Service Activator Feature	Cisco IOS Cartridge
multicastDevice Configuration Policy	●
multicastInterface Configuration Policy	●
multicastAutoRp Configuration Policy	●
multicastBootstrapRp Configuration Policy	●
multicastVrf Configuration Policy	●

VRF Route Maps

IP Service Activator Feature	Cisco IOS Cartridge
bgpRoutePolicy Configuration Policy	●
vrfRoutePolicy Configuration Policy	●

Interface Configuration Management

IP Service Activator Feature	Cisco IOS Cartridge
Subinterface Creation	
atmSubInterfaceData	●
frSubInterfaceData	●
vlanSubInterfaceData	●
Interface Decoration	
plPosInterfaceData	●
plSerialInterfaceData	●
ciscoUniversalInterface	●
ciscoEthernetPortCharacteristics	●
Interface Creation and Decoration	
loopbackInterfaceData	●
virtualTemplateInterface	●
basicRateInterfaceData	●
dialerInterface	●
multilinkInterface	●
Channelized Interface Creation	
e1ChannelizedInterface	●
e1Controller	●
e3ChannelizedSerialInterface	●
e3Controller	●
stm1ChannelizedSerialInterface	●
stm1Controller	●
t1ChannelizedSerialInterface	●
t1Controller	●
t3ChannelizedSerialInterface	●
t3Controller	●
Other	
backUpInterfacePolicy	●
dialerList	●
dlswDevice	●
dlswEthernetInterface	●
dlswTokenRingInterface	●
hsrp	●
pppMultilink	●
sgbp	●

Base Configuration Policies

IP Service Activator Feature	Cisco IOS Cartridge
banners Configuration Policy	●
ipPools Configuration Policy	●
keyChains Configuration Policy	●
prefixListEntries Configuration Policy	●
snmpCommunities Configuration Policy	●
snmpHosts Configuration Policy	●
staticRoutes Configuration Policy	●
userAuth Configuration Policy	●

userData Configuration Policy (provided for generic data model annotation only)	O

Unsupported features

The following features are not currently supported with the IP Service Activator Cisco IOS Cartridge:

Layer 2 VLL

VPLS

DU VPN

LSP

IPSec

Cisco hardware and software

Contact Oracle Global Customer Support (GCS) for the most up-to-date information about the supported Cisco devices. For Oracle GCS contact information, refer to the IP Service Activator *Release Notes*.

Operating systems

Refer to the IP Service Activator *Release Notes* for complete information about the operating systems supported for the Cisco IOS cartridge.

Installing the cartridge

Refer to the IP Service Activator *Setup Guide* for the cartridge installation and un-installation procedures.

Installing configuration policies

IP Service Activator supports extensible configuration policies that are seen through the GUI. Each configuration policy includes one CFG file and one or more zipped HTML files.

Refer to the IP Service Activator *Setup Guide* for the configuration policy installation procedure.

Refer to the IP Service Activator *Online Help* for more information on configuration policies, interface policy registration and interface/sub-interface creation.

Upgrading the Cisco IOS

This section explains the steps you need to perform before and after upgrading the Cisco IOS.

Prerequisites

Before performing the Cisco IOS upgrade, complete the following tasks for the device you are upgrading:

1. Ensure there are no concretes in a conflicted or disabled state on the device.
2. Run an audit to determine whether IP Service Activator and the device configuration are synchronized.
3. Stop all provisioning on the device.
4. Unmanage the device.

Upgrading

Refer to the Cisco documentation for instructions on upgrading the Cisco IOS.

Post-upgrade tasks

After performing the Cisco IOS upgrade, complete the following tasks for the device you have upgraded:

1. Reset the device capabilities:

   Right-click on the device and select **Properties**

   Select the **Capabilities** page

   Click **Reset Device Capabilities**

   In the confirmation popup, click **Yes**

   Click OK and then **Commit**
2. Rediscover the device: right-click on the device and select **Discover**.
3. Look in the device properties file to verify that the new IOS version was picked up by IP Service Activator: right-click on the device and select **Properties** – the **Description** field displays the new IOS version.
4. Manage the device and set it to offline maintenance mode:

   Right-click on the device and select **Properties**

Select the Management page

On the **Command Delivery** menu, select **Offline Maintenance**

Right-click on the device and select **Manage**

Click **OK** and then **Commit**

You can access the audit log at the following location to confirm commands were processed in offline maintenance mode:

/opt/OracleCommunications/IPServiceActivator/AuditTrails/npCisco.audit.log

You can also access the network processor logs to confirm processing of the configuration after managing the device:

/opt/OracleCommunications/IPServiceActivator/logs/networkprocessor.log

When you manage the device in offline maintenance mode, the following message appears in the fault pane for concretes associated with the managed device:

"Changes to configuration were attempted while in an Offline Mode; some configuration has not been applied to the device"

You can safely ignore this message.

5. Change the command delivery mode for the device to online: right-click on the device and select **Command Delivery** > **Online** and then **Commit**.

6. Run an audit to verify that IP Service Activator and the device configuration are synchronized:

   Right-click on the device and select **Properties**

   Select the Audit/Migrate page

   Click the **Initiate Audit** button

   When the audit is finished, click **Detach Audit**. Then right-click in the new window that appears, choose **Select All** and copy-paste the text to another application or file.

The device is ready for provisioning through IPSA.

Note: If the audit fails and the post-upgrade audit results show discrepancies between the IP Service Activator configuration and the device configuration, you must verify and update the Cisco IOS options using the IP Service Activator Cisco IOS Cartridge Configuration Tool, which shows you the options available for your device and IOS combination – see Cisco Cartridge Configuration Utility. For additional help, you can contact Oracle Global Customer Support – see Contacting Oracle Global Customer Support (GCS).

Device Configuration

Supported authentication methods

The supported authentication methods are listed in the following table:

Device Access		All Devices
Telnet	TACACS+	✓
	None	
	Named User	
	Anonymous	✓
	SNMPv1	
	SNMPv2c	
	Password only	
SSH	SSH with password authentication	✓
	SSH with keyed authentication	

Note: Anonymous without enable is invalid for Cisco.

Manual pre-configuration

To discover a device, the routers must have few manual SNMP parameters created when a new device is added to a network.

To configure the necessary functionality on the device, refer to Cisco documentation – go to http://www.cisco.com/public/support/tac/documentation.html.

Sample configuration

The following is a sample Cisco device configuration:

```
Current configuration : 13567 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
service password-encryption
!
hostname rot7206-5
!
boot-start-marker
boot system disk0:c7200-spservicesk9-mz.124-2.T3.bin
boot-end-marker
!
logging snmp-authfail
logging buffered informational
enable secret 5 $1$QimD$rkbKm99WWdUb2tgJ7g7t20
!
aaa new-model
!
!
aaa authentication login default group radius local line
aaa authentication login con line
aaa authentication login h323 group radius
!
ip subnet-zero
ip cef

snmp-server community public RO
!
line con 0
 exec-timeout 20 0
 privilege level 4
 password 7 060A0E23
 login authentication con
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
```

```
 exec-timeout 45 0
 password 7 0703204E
 rotary 1
!
```

Cisco Cartridge Configuration Utility

The IP Service Activator Cisco IOS Cartridge configuration utility is a command line tool that is installed with the Cisco IOS Cartridge, and provides the ability to automatically generate options and registry files for your Cisco devices.

You can run the Cisco cartridge configuration utility to generate a CSV (comma-separated values) file of all the Cisco devices and IOS combinations in your IP Service Activator database. You can then run the Cisco cartridge configuration utility again to generate the options files for your devices. The Cisco cartridge configuration utility reads the options from the master options CSV file and matches them to your device and IOS combinations. The Cisco cartridge configuration utility will create an options *xml* file for each device and IOS version. The tool can be run with a different parameter to generate a registry file that will use the newly generated options files. The necessary procedures are provided in this section, and cover the tasks listed in the task checklist.

Task checklist

The following list displays the suggested order of tasks for using the Cisco cartridge configuration utility:

1. Using the Cisco cartridge configuration utility: general commands
2. Retrieving a list of device type and IOS version combinations
3. Generating the registry file
4. Generating multiple options files and/or Generating a single options file
5. Generating capabilities files

Using the Cisco cartridge configuration utility: general commands

The Cisco cartridge configuration utility is installed with the IP Service Activator Cisco IOS Cartridge and it is located in the *<SERVICE_ACTIVATOR_HOME>/bin* directory.

The following table displays general usage commands for the Cisco cartridge configuration utility.

Command	Description
-generateCapabilitiesFiles	Generates an initial set of capabilities files
-generateOptionsInDir	Generates the complete set of options in the output directory

-generateOptionsZip	Generates the complete set of options
-generateRegistry	Generates the **MIPSA_registry.xml** file
-generateSingleOptionsFile	Generates a single options file
-help	Displays help text for the Cisco cartridge configuration utility
-output	Sets the output filename or directory
-queryActiveDeviceTypesAndIOS	Queries IP Service Activator for active Cisco device and IOS data

Retrieving a list of device type and IOS version combinations

To retrieve a list of device type and IOS version combinations:

1. Navigate to the <*SERVICE_ACTIVATOR_HOME*> directory.
2. Execute one of the following commands:

   bin/cartridgeConfigurationTool.sh –queryActiveDeviceTypesAndIOS db [<*host name*> <*port*> <*sid*> <*user name*> <*password*>**] [proxyagent] [-output** <*output_filename*>**]**

   OR

   bin/cartridgeConfigurationTool.sh -queryActiveDeviceTypesAndIOS oim [<*hostname*> <*port*> <*username*> <*password*>**] [proxyname] [-output** <*output_filename*>**]**

Where	Is
db	Used to query data directly from the database
oim	Used to query data via the IP Service Activator Integration Manager
<*hostname*>	The database (db) or IP Service Activator naming service (oim) host name or IP address
<*port*>	The database (db) or IP Service Activator naming

	service (oim) port number. (Optional)
<*sid*>	The database (db) SID
<*username*>	The database (db) or IP Service Activator (oim) username
<*password*>	The database (db) or IP Service Activator (oim) password
<*proxyagent*>	Used to restrict the device query to devices managed by the specified proxy agent (optional)
<*output_filename*>	The device IOS data output file (optional) that will be created in <*SERVICE_ACTIVATOR_HOME*> directory

For example:

bin/cartridgeConfigurationTool.sh -queryActiveDeviceTypesAndIOS oim localhost 2809 orchestream orchestream -output device_ios.csv

Generating the registry file

Using the Cisco cartridge configuration utility, you can generate the **MIPSA_registry.xml** file with your set of device type and IOS version combinations.

To generate the registry file:

1. Navigate to the <*SERVICE_ACTIVATOR_HOME*> directory.
2. Execute the following command:

bin/cartridgeConfigurationTool.sh -generateRegistry <*device_ios_data*> <*package*> **default|series|device|deviceios [-output** <*output_filename*>**]**

Where	Is
<*device_ios_data*>	The csv file of the device type and IOS version pairs that was generated in the procedure Retrieving a list of device type and IOS version combinations
<*package*>	The package prefix for options and capabilities files
default	Used to generate all capabilities references to **cisco_default.xml**
series	Used to generate capabilities references for each device series – for example: **cisco_3600.xml**

device	Used to generate capabilities references for each device type – for example: **cisco_3640.xml**
deviceios	Used to generate capabilities references for each device IOS combination – for example: **cisco_3640-12.2(13)T.xml**
<*output_filename*>	The name of the output registry file

For example:

bin/cartridgeConfigurationTool.sh -generateRegistry device_ios.csv com.oracle.ipsa series -output MIPSA_registry.xml

The **MIPSA_registry.xml** file is saved in the <*SERVICE_ACTIVATOR_HOME*> directory.

3. Copy the generated registry file to the following directory:

<*SERVICE_ACTIVATOR_HOME*>**/Config/networkProcessor**

Note: If you need to re-generate the **MIPSA_registry.xml** file by running this procedure again at a later time, you must re-start the Network Processor or reload the registry after completing this procedure. When you reload the registry, the Network Processor reloads its configuration files. The path for reload registry is <*SERVICE_ACTIVATOR_HOME*>/bin. To reload the registry, execute the following command:

npAdmin.sh reload_registry

Understanding registry file behavior

An entry in the **MIPSA_registry.xml** file matches a device if **all** of the following conditions are met:

driverType is equal to the “Device Driver” value from the **Device Type** entry on the Topology tab in the IP Service Activator GUI

deviceType is equal to the “Model, s/w Vn” value from the **Device Type** entry on the Topology tab in the IP Service Activator GUI

osVersion appears as a substring in the **Description** field on the device property page in the IP Service Activator GUI

If multiple entries in the **MIPSA_registry.xml** file match a given device, the first entry (the one listed first in the file) is used.

Regular expression matching is not supported for the **driverType** field. However, it can be enabled for the **deviceType** and **osVersion** fields by including the **useRegex** attribute as follows:

<deviceType useRegex="true" >Cisco 2611</deviceType>

<osVersion useRegex="true" >12.2(15)T16</osVersion>

See the sample **MIPSA_registry.xml** file below for examples of the values mentioned above.

Sample registry file entry

The following is a sample MIPSA registry file entry:

```
<!-- Cisco 2611 -->
<cartridgeUnit>
<name>com.oracle.ipsa.cu1.2611.12.2(15)T16</name>
<driverType>cisco</driverType>
<deviceType>Cisco 2611</deviceType>
<osVersion>12.2(15)T16</osVersion>
<smToDmQuery>com/metasolv/serviceactivator/cartridges/cisco/units/cu1/sm2dm.xq</smToDmQuery>
<dmValidation>com/metasolv/serviceactivator/cartridges/cisco/units/cu1/dmValidation.xq</dmValidation>
<dmMigration>com/metasolv/serviceactivator/cartridges/cisco/xquerylib/dmMigration.xq</dmMigration>
<dmToCliQuery>com/metasolv/serviceactivator/cartridges/cisco/units/cu1/annotatedDm2Cli.xq</
dmToCliQuery>
<capabilities>com/oracle/ipsa/capabilities/cisco_2600.xml</capabilities>
<options>com/oracle/ipsa/options/Cisco_2611-12.2(15)T16.xml</options>
<errorMessages>com/metasolv/serviceactivator/cartridges/cisco/messages/errorMessages.xml</
errorMessages>
<warningMessages>com/metasolv/serviceactivator/cartridges/cisco/messages/warningMessages.xml</warning
Messages>
<successMessages>com/metasolv/serviceactivator/cartridges/cisco/messages/successMessages.xml</success
Messages>
</cartridgeUnit>
```

Generating multiple options files

Using the Cisco cartridge configuration utility, you can generate a complete set of options configuration files for your Cisco device types and IOS versions.

To generate multiple options files:

1. Navigate to the *<SERVICE_ACTIVATOR_HOME>/lib/java-lib/cartridges/cisco* directory.

2. Execute the following command:

   bin/cartridgeConfigurationTool.sh -generateOptionsZip *<options_filename>* *<device_ios_data>* *<package>* **-output** *<output_zipfile>*

Where	Is
<options_filename>	The path to the master options configuration data (**cisco_options.csv**)
<device_ios_data>	The csv file of the device type and IOS version pairs that was generated in the procedure Retrieving a list of device type and IOS

	version combinations
<package>	The package prefix for options files
<output_zipfile>	The file name of the output zip file

For example:

bin/cartridgeConfigurationTool.sh -generateOptionsZip Config/cisco_options.csv device_ios.csv com.oracle -output cisco_options.zip

The **cisco_options.zip** file is saved in the *<SERVICE_ACTIVATOR_HOME>lib/java-lib/cartridges/cisco* directory.

To load the updated options, perform one of the following steps:

3. Extract the **cisco_options.zip** file to the **<SERVICE_ACTIVATOR_HOME>/Config/networkProcessor** directory. The new options will be dynamically picked up from the classpath if you use the reload_registry command.

Alternatively,

4. Shut down and restart the network processor. The updated options will be reloaded from the options.zip file.

Note: If you need to re-generate options by running this procedure again at a later time, you must re-start the Network Processor after completing this procedure.

Generating a single options file

Using the Cisco cartridge configuration utility, you can generate a single options file for a specific Cisco device type and IOS version.

To generate a single options files:

1. Navigate to the *<SERVICE_ACTIVATOR_HOME>* directory.

2. Execute the following command:

   bin/cartridgeConfigurationTool.sh -generateSingleOptionsFile *<options_filename> <device_type> <ios_version>* **[-output** *<output_filename>***]**

Where	Is
<options_filename>	The path to the master options configuration data file (**cisco_options.csv**)

<*device_type*>	The Cisco device type
<*ios_version*>	The Cisco IOS version
<*output_filename*>	The name of the output xml file

For example:

bin/cartridgeConfigurationTool.sh -generateSingleOptionsFile Config/cisco_options.csv "Cisco 3640" 12.2(13)T4 –output cisco_options_3640_12.2(13)T4.xml

The generated file is saved in the <*SERVICE_ACTIVATOR_HOME*> directory.

3. Copy the output xml file to the following directory:

<*SERVICE_ACTIVATOR_HOME*>**/Config/networkProcessor/com/oracle/ipsa/options**

Note: If you need to re-generate options by running this procedure again at a later time, you must re-start the Network Processor or reload the registry after completing this procedure. When you reload the registry from <*SERVICE_ACTIVATOR_HOME*>**/bin**, the Network Processor reloads its configuration files. To reload the registry, execute the following command:

npAdmin.sh reload_registry

Generating capabilities files

Using the Cisco cartridge configuration utility, you can generate an initial set of capabilities files based on the default cartridge capabilities.

Note that only new (missing) capabilities files are generated – existing files are not modified.

To generate capabilities files:

1. Navigate to the <*SERVICE_ACTIVATOR_HOME*> directory.

2. Execute the following command:

bin/cartridgeConfigurationTool.sh -generateCapabilitiesFiles <*device_ios_data*> <*package*> **default|series|device|deviceios [-output** <*output_dir*>**]**

Where	Is
<device_ios_data>	The csv file of the device type and IOS version pairs that was generated in the procedure Retrieving a list of device type and IOS version combinations
<package>	The package prefix for capabilities files
default	Used to generate the capabilities file **cisco_default.xml**
series	Used to generate the capabilities files for each device series – for example: **cisco_3600.xml**
device	Used to generate the capabilities files for each device type – for example: **cisco_3640.xml**
deviceios	Used to generate the capabilities files for each device IOS combination – for example: **cisco_3640-12.2(13)T.xml**
<output_directory>	The directory where the capabilities package and files are to be created (optional) – if you do not specify a directory, IP Service Activator will use the current directory.

For example:

bin/cartridgeConfigurationTool.sh -generateCapabilitiesFiles device_ios.csv com.oracle series -output ./Config/networkProcessor

The Cisco cartridge configuration utility creates the capabilities file and places it in a package directory structure in the following directory:

*<SERVICE_ACTIVATOR_HOME>***/Config/networkProcessor/com/oracle/ipsa/capabilities**

Note: If you need to re-generate the capabilities files by running this procedure again at a later time, you must re-start the Network Processor or reload the registry after completing this procedure. When you reload the registry from <SERVICE_ACTIVATOR_HOME>**/bin**, the Network Processor reloads its configuration files. To reload the registry, execute the following command:

npAdmin.sh reload_registry

Cisco Pre-checks

The pre-checks look for existing configuration on a device when you commit a configuration. This prevents the breaking of any existing services.

During creation of a new service instance by IP Service Activator, pre-checks are executed to determine if IP Service Activator configuration will create any conflicts with existing configuration. If such a condition is detected the operation is aborted and an error message in generated.

Installing pre-checks

The standard pre-checks are installed when IP Service Activator is installed. For more information see the IP Service Activator *Setup Guide*.

Enabling/disabling pre-checks

By default, some pre-checks are in enabled state and some of them are in disabled state. However, you can change any one of them using the **standard.properties** file. The file is located in the following directory:

Config/networkProcessor/com/metasolv/serviceactivator/cartridges/cisco/pre_check/standard.properties.txt

To disable a particular pre-check change its value to *false*, as shown in the example below. The value **true** indicates an enabled pre-check.

```
<checkProperties xmlns="http://www.metasolv.com/
serviceactivator/checkproperties" >
    <preCheckRouteMap>true</preCheckRouteMap>
    <preCheckClassMap>true</preCheckClassMap>
    <preCheckPolicyMap>true</preCheckPolicyMap>
    <preCheckNamedAcl>true</preCheckNamedAcl>
    <preCheckVrf>true</preCheckVrf>
    <preCheckCryptoMap>true</preCheckCryptoMap>
    <preCheckConfigVersion>false</preCheckConfigVersion>
    <preCheckRouterIOSUpgrade>false</preCheckRouterIOSUpgrade>
    <preCheckPolicer>true</preCheckPolicer>
</checkProperties>
```

Individual pre-checks

This section outlines the behavior of the individual pre-checks for the Cisco IOS Cartridge.

Name	Behavior	Default
preCheckRouteMap	Raises a fault when a route map with the specified name exists. It is a VPN service pre-check.	On
preCheckClassMap	Raises a fault when a class map with the specified name exists. It is a QOS service pre-check.	On
preCheckPolicyMap	Raises a fault when a policy map with the specified name exists. It is a QOS service pre-check.	On
preCheckCryptoMap	Raises a fault when a crypto map with the specified name and sequence exists. It is a IPSec service pre-check.	On
preCheckNamedAcl	Raises a fault when an ACL with the specified name exists. It is a QoS service pre-check.	On
preCheckVrf	Raises a fault when a VRF with the specified name exists. It is a VPN service pre-check.	On
preCheckRouterIOSUpgrade	Raises a fault when router IOS version does not match the version from the last device discovery.	Off
preCheckConfigVersion	Raises a fault when the IP Service Activator and the router configuration versions do not match.	Off
preCheckPolicer	Raises a fault when an aggregate policer with the specified name exists. It is a Layer 2 QOS service pre-check.	On
preCheckMlsQos	Raises a fault when MLS QoS is disabled. It is a Layer 2 QoS service pre-check.	Off
preCheckVlanVtpModeServer	Raises a fault when the user tries to add a VLAN with value greater than 1005 while router runs in VTP Server mode. It is a VLAN service pre-check.	On
preCheckVlanVtpModeClient	Raises a fault when the user tries to add or modify a VLAN while router runs in VTP Client mode. This pre-check, looks for any VLAN operations involving adding new VLAN, and modifying or deleting any existing VLAN. If enabled, it takes over pre-checking transactions of the preCheckVlanVtpModeServer pre-check.	Off

	for the extended VLAN range with IDs above 1005. It is a VLAN service pre-check.	
preCheckInterfaceMediaType	Raises faults in the following scenarios: ▪ interface media type is RJ45 and speed is being set to default or nonegotiate value. ▪ interface media type is not RJ45 and speed is not being set to default or nonegotiate value. **Note**: This pre-check is only invoked when a user tries to set GigabitEthernet interface Speed value through ciscoEthernePortCharacteristics configuration policy.	On
VRF Preservation	VRF-Preservation, including preservation of route map configuration when manually configured sites are detected. This is determined by the presence of additional prefix-list entries.	On
VRF-RDConflict	Detects an attempt to change RD	On
ExportRouteMapNameConflict	Detects conflicting Export Route Map Name	On
RouteMapConflict	Detects conflicting Managed Match and Set Action	On
Additional RouteMapMatchCriteria	Detects unrecognized match statement in route-map	On
AdditionalRouteMapSetActions	Detects unrecognized set statement in route-map	On
PrefixListConflict	Detects conflicting Prefix List contents	On

Appendix A: Options Framework

By using the options framework in the Cisco IOS Cartridge, you can control the variations in configuration style for different device types and IOSs. These options are registered by the cartridge in the **MIPSA_registry.xml** file. A sample file is displayed below:

```
…
<!-- Cisco 2611 -->
<cartridgeUnit>
  <name>com.oracle.ipsa.cu5.2611</name>
  <driverType>cisco</driverType>
  <deviceType>Cisco 2611</deviceType>
  <osVersion>12.0(7)T</osVersion>
  <smToDmQuery>com/metasolv/serviceactivator/cartridges/cisco/units/cu5/sm2dm.xq</smToDmQuery>

<dmValidation>com/metasolv/serviceactivator/cartridges/cisco/units/cu5/dmValidation.xq</dmVali
dation>

<dmMigration>com/metasolv/serviceactivator/cartridges/cisco/xquerylib/dmMigration.xq</dmMigrat
ion>

<dmToCliQuery>com/metasolv/serviceactivator/cartridges/cisco/units/cu5/annotatedDm2Cli.xq</dmT
oCliQuery>
  <capabilities>com/oracle/ipsa/capabilities/cisco_default.xml</capabilities>
  <options>com/oracle/ipsa/options/Cisco_2611-12.0(7)T.xml</options>

<warningMessages>com/metasolv/serviceactivator/cartridges/cisco/units/cu5/warningMessages.xml<
/warningMessages>
</cartridgeUnit>
…
```

The **<options>** entry references an option configuration file in the **classpath** application.

For example, the file **Cisco_2611-12.0(7)T.xml** is located in the following directory:

<SERVICE_ACTIVATOR_HOME> **/Config/networkProcessor/com/oracle/ipsa/options**

A sample file is displayed below:

```
<base:options xsi:type="CartridgeOptions"
xmlns="http://www.metasolv.com/serviceactivator/cisco/options"
xmlns:base="http://www.metasolv.com/serviceactivator/options"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">


<cartridge.cisco.qos.mapClassNamingStrategy>auto</cartridge.cisco.qos.mapClassNamingStrategy>
<cartridge.cisco.qos.atmQosOnPvc>vcClass</cartridge.cisco.qos.atmQosOnPvc>


</base:options>
```

Configuration options

The following table lists the configuration options for the Cisco IOS Cartridge. Oracle recommends configuring the options at deployment. The default value is used if an options entry is not defined.

Note:

1. For the options files to be valid, you must enter the options definitions in the order documented below.
2. If you change an option value for a device that has existing configurations provisioned by IP Service Activator, the configurations are removed and re-added using the new configuration style.

Option	Default Value	Description	SM2DM	DM2CLI
cartridge.cisco.qos. mapClassNamingStrategy	auto	Cisco Map Class Naming Strategy Defines the Frame Relay map class naming strategy: auto (default) - auto generate the name concatenation - creates the map-class name by concatenating the names of all PHB groups (PHB or/and MQC) applied to the interface, both inbound and outbound. For example, if two PHB groups called FRTSPHBgroup and MQCOut are applied to an interface, the map-class command would be as follows: map-class frame-relay FRTSPHBGroup-MQCOut phbname - name the map-class after one of the PHB and MQC PHB groups that contribute to the map-class.	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		Take the name from the following list in the specified order: o PHB group (if it exists) o outbound MQC PHB group (if it exists) o inbound MQC PHB group		
cartridge.cisco.qos.mapclass.framerelay.mincir.in.validation	sameAsOut	Cisco Map Class Frame Relay mincir in validation Defines the type of validation for the Frame Relay mincir in value. sameAsOut (default) - the mincir in value needs to be equal to the mincir out value noValidation - no validation will be done for the mincir in value	Supported	Not supported
cartridge.cisco.qos.atmQosOnPvc	vcClass	Cisco ATM QOS on PVC Defines how QOS is provisioned on ATM PVCs: vcClass (default) - use the VC class direct - provision directly on PVC	Supported	Not supported
cartridge.cisco.qos.trafficShapingOnFRInterface	mapClass	Cisco Traffic Shaping on Frame Relay Interface Defines how traffic shaping is provisioned on Frame Relay interfaces: policyMap - use a	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		policy map mapClass (default) - use a map class dts - use distributed traffic shaping (7500 series)		
cartridge.cisco.qos. suppressRateLimitAcl	false	Cisco Suppress Rate Limit ACL Indicates whether the access group in the rate-limit command should be suppressed when no classification is used.	Supported	Not supported
cartridge.cisco.qos.ratePoliceFormat	multiLine	Cisco Rate Policing Format Indicates which command format to use: singleLine - use single line format multiLine (default) - use multiple line format	Supported	Not supported
cartridge.cisco.qos.policymap.police. defaultCBSValue	-1	Cisco Police CBS Default Value Indicates the Committed Burst Size to use when the default checkbox is checked in the MQC PHB Group Police tab. The value must be greater than -1 in order to take effect. If a negative value is specified, the CBS value is not configured when the "police" command is issued.	Supported	Not supported
cartridge.cisco.qos.policymap.police.defaultEBSValue	-1	Cisco Police EBS Default Value	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		Indicates the Excess Burst Size to use when the default checkbox is checked in the MQC PHB Group Police tab. The value must be greater than -1 in order to take effect. If a negative value is specified, the EBS value is not be configured when the "police" command is issued.		
cartridge.cisco.qos.classmap.dscpMatchEnhanced	false	Cisco Class Map Match IP DSCP Enhanced Indicates which command format to use: true: match dscp [IPv4 and IPv6 packets] false: match ip dscp [IPv4 packets only] This option also applies during strict aggregation. This option only applies	Supported	Not supported
cartridge.cisco.qos.classmap.precedenceMatchEnhanced	false	Cisco Class Map Match IP Precedence Enhanced Indicates which command format to use: true: match precedence [IPv4 and IPv6 packets] false: match ip precedence [IPv4 packets only]This option also applies during strict aggregation.	Supported	Not supported
cartridge.cisco.qos.classmap.tosType	object-model	Cisco Class Map TOS Type Indicates the TOS to use when issuing the classmap command of “match [dscp | precedence]”:	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		object-model: packet marking is dictated by the object model dscp: dscp marking is used, similar to the ClassMap_DscpMatch setting in the CDD mechanism file precedence: precedence marking is used This option also applies during strict aggregation.		
cartridge.cisco.qos.classmap.existWithEmptyMatchCriteria	true	Cisco Class Map Exists with Empty Match Criteria Indicates whether the device allows a class map to exist without any match criteria: true: class maps can exist without any match criteria false: class maps can't exist without any match criteria If the value is set to “false”, you must ensure that a modification to the class map does not result in all of its match criteria being removed. In some cases, you may need to remove the service policy from the interface in order for the operation to be successful.	Not supported	Supported
cartridge.cisco.qos.classmap.matchany.isSupported	true	Cisco Catalyst Switches Support for the Match Any Command Indicates if the "match any" command is	Not supported	Supported

Option	Default Value	Description	SM2DM	DM2CLI
		supported for class map configurations: true: create the class map with a "match any" statement false: create the class map without a “match any” statement Strict aggregation does not change the behavior of this option. Changing this value changes support for "match any" commands.		
cartridge.cisco.qos.policymap.fairqueue.isSupported	true	Cisco Support for the Fair-Queue Command Indicates if the "fair-queue" command is supported for policy map configurations: true: create the policy map with a "fair-queue" statement false: no ACL reference; "fair-queue" statements are used in the policy map Changing this value changes support for "fair-queue" commands.	Supported	Not supported
cartridge.cisco.qos.policymap.setDscpEnhanced	false	Cisco Policy Map Set IP DSCP Enhanced Indicates which command format to use: true: set dscp [IPv4 and IPv6 packets] false: set ip dscp [IPv4 packets only]	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
cartridge.cisco.qos.policymap.setPrecedenceEnhanced	false	Cisco Policy Map Set IP Precedence Enhanced Indicates which command format to use: true: set precedence [IPv4 and IPv6 packets] false: set ip precedence [IPv4 packets only]	Supported	Not supported
cartridge.cisco.qos.policymap.setTosType	object-model	Cisco Policy Map Set TOS Type Indicates which type of packet marking to use in the policy-map command: object-model: packet marking is dictated by the object model dscp: dscp marking is used, similar to the PolicyMap_SetDscp setting in the CDD mechanism file precedence: precedence marking is used	Supported	Not supported
cartridge.cisco.multicast.distributedSwitching	unsupported	Cisco Muticast Routing Distributed Keyword Indicates whether multicast distributed switching is mandatory, optional, or not supported on the device.	Supported	Not supported
cartridge.cisco.qos.policymap.defaultWREDType	dscp	Cisco Default WRED Type for Policy Map Indicates which WRED type to use by default in policy map configuration	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		mode: dscp: issues the command “random-detect dscp-based” precedence: issues the command “random-detect precedence”		
cartridge.cisco.qos.policymap.wredType	object-model	Cisco WRED Type for Policy Map Indicates which packet marking to use in policymap WRED commands (MQC WRED in IP Service Activator): object-model: packet marking is dictated by the object model dscp: dscp marking is used, similar to the PolicyMap_DiffservCompliantWred setting in the CDD mechanism file precedence: precedence marking is used	Supported	Not supported
cartridge.cisco.qos.phbwfq.dropStrategy.wredType	object-model	Cisco Drop Strategy as WRED for PHB WFQ Indicates which packet marking to use in policymap random detect commands (phb wfq in IP Service Activator): object-model: object model decides packet marking dscp: uses dscp marking precedence: uses precedence marking	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
cartridge.cisco.qos.phbwfq.dropStrategy.defaultWREDType	dscp	Cisco Drop Strategy as defaultWRED for PHB WFQ Indicates which packet marking to use in policymap random detect commands (phb wfq in IP Service Activator): dscp: issues the command "random-detect dscp-based" precedence: issues the command "random-detect precedence"	Supported	Not supported
cartridge.cisco.qos.policymap.wredDscpGsrBug	false	Cisco Generate Extra Random-Detect Command for Dscp Indicates whether to issue an extra "random-detect" command for DSCP based policy maps. This can be used for devices that have problems with the normal "random-detect" command sequence, such as GSRs running IOS 12.0(*)S: true: an extra "random-detect" command is issued – "random-detect" and "random-detect dscp-based" false: the "random-detect dscp-based" command is issued	Not supported	Supported
cartridge.cisco.qos.interface.wredType	object-model	Cisco Interface WRED Type Indicates which packet marking to use in interface WRED commands (PHB WRED in IP Service Activator):	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		object-model: packet marking is dictated by the object model dscp: dscp marking is used, similar to the Wred_DiffservCompliantWred setting in the CDD mechanism file precedence: precedence marking is used		
cartridge.cisco.qos.car.setTosType	object-model	Cisco CAR Set TOS Type Indicates which type of packet marking to set in the rate limit command (policing rule in IP Service Activator): object-model: packet marking is dictated by the object model dscp: dscp marking is used, similar to the Car_SetDiffServ setting in the CDD mechanism file precedence: precedence marking is used	Supported	Not supported
cartridge.cisco.qos.acl.numbered.tosType	object-model	Cisco Numbered ACL TOS Type Indicates which type of packet marking to use in the numbered ACL command: object-model: packet marking will be decided by the object model dscp: dscp marking will be used, similar to the NumberedAcl_Dscp setting in the CDD mechanism file	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		precedence: precedence marking will be used		
cartridge.cisco.qos.acl.named.tosType	object-model	Cisco Named ACL TOS Type Indicates which type of packet marking to use in the named ACL command: object-model: packet marking is dictated by the object model dscp: dscp marking is used, similar to the NamedAcl_Dscp setting in the CDD mechanism file precedence: precedence marking is used	Supported	Not supported
cartridge.cisco.qos.acl.protocolFor94	nos	Cisco protocol name for protocol no. 94 Indicates whether to send ipinip or nos for protocol 94.	Not supported	Supported
cartridge.cisco.qos.policymap.police.tosType	object-model	Cisco Policy Map Police TOS Type Indicates which type of police action you select for MQC policing: object-model: the police action is decided by the object model dscp: the 'set-dscp-transmit' action is used precedence: the 'set-prec-transmit' action is used	Supported	Not supported
cartridge.cisco.qos.policymap.	false	Cisco CIR Value is	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
police.roundoffCIRValue		Rounded Up Indicates whether the device rounds the CIR value upwards in "police or mls qos aggregate-policer" commands. If the value is set to 'true', the cartridge rounds the CIR value upwards. It uses the 'cartridge.cisco.qos.policymap.police.roundoffCIRFactor' option in order to determine the nearest multiple to round towards.		
cartridge.cisco.qos.policymap.police.roundoffCIRFactor	8000	Cisco Multiple Used when Rounding CIR Values This value indicates the multiple that the device uses when rounding up CIR values in "police or mls qos aggregate-policer" commands. The cartridge rounds the CIR value upwards to the nearest multiple of the specified value. The 'cartridge.cisco.qos.policymap.police.roundoffCIRValue' option must be set to 'true' in order for this value to take effect.	Supported	Not supported
cartridge.cisco.qos.policymap.police.violateAction.isSupported	true	Cisco Support for the Police Violate Action Indicates whether the "violate-action" parameter is supported for the police command. If this value is set to 'false', then the "violate-action" parameter is not issued.	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
cartridge.cisco.qos.policymap.police.conformAction.isSupported	true	Cisco Support for the Police Conform Action Indicates whether the "conform-action" parameter is supported for the police command. If this value is set to 'false', then the "conform-action" parameter is not issued.	Supported	Not supported
cartridge.cisco.qos. rateLimitWithMplsAction	set-mpls-exp	Cisco Rate Limit MPLS Action Indicates which MPLS Action to use: set-mpls-exp-imposition: use mpls imposition set-mpls-exp (default): use multiple line format	Supported	Not supported
cartridge.cisco.qos. sendAllShapeRates	false	Cisco Shape Rates Indicates which command format to use: For Average shaping: o shape average {cir} or shape average {cir} {cir*4ms} {cir*4ms} eg. shape average 56000 or shape average 56000 224 224 o shape average {cir} {bc} or shape average {cir} {bc} {bc} eg. shape average 56000	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		28000 or shape average 56000 28000 28000 For Peak Shaping: o shape peak {cir} or shape peak {cir} {cir*4ms} {cir*4ms} eg. shape peak 16000 or shape peak 16000 64 64 o shape peak {cir} {bc} or shape peak {cir} {bc} {bc} eg. shape peak 56000 28000 or shape peak 56000 28000 28000		
cartridge.cisco.qos.atmHoldQueue.maximum	1024	Cisco QOS ATM Hold Queue Depth Maximum Value Defines the maximum value for the ATM Hold Queue Depth. A fault is raised if the ATM Hold Queue Depth is greater than the specified value.	Supported	Not supported
cartridge.cisco.qos.atmHoldQueue.minimum	5	Cisco QOS ATM Hold Queue Depth Minimum Value Defines the minimum value for the ATM Hold Queue Depth. A fault is raised if the ATM Hold Queue Depth is less than the specified value.	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
cartridge.cisco.qos.atmPvcVciRange.maximum	1023	Cisco QOS ATM PVC VCI Maximum Value Defines the maximum value for the ATM PVC VCI. A fault is raised if the ATM PVC VCI is greater than the specified value.	Supported	Not supported
cartridge.cisco.qos.atmPvcVciRange.minimum	0	Cisco QOS ATM PVC VCI Minimum Value Defines the minimum value for the ATM PVC VCI. A fault is raised if the ATM PVC VCI is less than the specified value.	Supported	Not supported
cartridge.cisco.qos.frHoldQueue.maximum	1024	Cisco QOS FR Hold Queue Depth Maximum Value Defines the maximum value for the Frame Relay Hold Queue Depth. A fault is raised if the Frame Relay Hold Queue Depth is greater than the specified value.	Supported	Not supported
cartridge.cisco.qos.frHoldQueue.minimum	1	Cisco QOS FR Hold Queue Depth Minimum Value Defines the minimum value for the Frame Relay Hold Queue Depth. A fault is raised if the Frame Relay Hold Queue Depth is less than the specified value.	Supported	Not supported
cartridge.cisco.qos.mlsQos.enable	false	Cisco Support for the "mls qos" Command Indicates whether the	Supported	Supported

Option	Default Value	Description	SM2DM	DM2CLI
		"mls qos" command can be used to enable QoS for the device.		
cartridge.cisco.qos.policingRule.rateLimit.roundoffCIRValue	true	Cisco CIR Value is Rounded Up Indicates whether the device rounds the CIR value upwards in “rare-limit output/input access-group” commands. If the value is set to ‘true’, then the cartridge will round the CIR upwards. The cartridge will use the ‘’cartridge.cisco.qos.policingRule.rateLimit.roundoffCIRFactor’’ option in order to determine the nearest multiple to round towards.	Supported	Not supported
cartridge.cisco.qos.policingRule.rateLimit.roundoffCIRFactor	8000	Cisco Multiple Used when Rounding CIR Values Indicates the multiple which the device uses when rounding up CIR values in “rate-limit output/input access-group” commands. The cartridge will round the CIR value upwards to the nearest multiple of the specified value. The “cartridge.cisco.qos.policingRule.rateLimit.roundoffCIRValue” option must be set to ‘true’ for this value to take effect.	Supported	Not supported
cartridge.cisco.saa.icmpEcho.sourceIpAddress.isSupported	true	Cisco Support for the SAA ICMP Echo Operation Source IP Address. Indicates whether the "Source IP Address" configuration is supported for SAA ICMP Echo	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		operations. A fault is raised if this value is set to 'false' and a source IP address is set for an ICMP Echo operation.		
cartridge.cisco.saa.tos.isSupported	true	Cisco Support for SAA ToS Indicates whether the "ToS" configuration is supported for SAA operations. A fault is raised if this value is set to 'false' and a ToS value is set for an SAA operation.	Supported	Not supported
cartridge.cisco.saa.rtr.schedule.forever.isSupported	true	Cisco Support for SAA Rtr-Schedule Lifetime Forever Indicates whether the "life forever" parameter is supported for the "rtr schedule" command. If the value is set to 'true', then the "life forever" parameter is used whenever the lifetime value is set to "Default".	Supported	Not supported
cartridge.cisco.saa.verifyErrorEnable.isSupported	true	Cisco Support for SAA Verify-Error-Enable with Error Checking Indicates whether the "verify-error-enable" parameter is supported for the "rtr reaction-configuration" command. A fault is raised if this value is set to 'false' and error checking is enabled.	Supported	Not supported
cartridge.cisco.saa.tcp.requestDataSize.isSupported	true	Cisco Support for SAA TCP Connect Operation	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		Request Data Size Indicates whether the "request-data-size" command is supported for SAA TCP Connect operations. A fault is raised if this value is set to 'false' and a request size is set for a TCP Connect operation.		
cartridge.cisco.saa.rtr.reactionConfig.upperThreshhold.isSupported	false	Cisco Support for SAA Upper-Threshold Parameter Indicates whether the "upper-threshold" parameter is supported for the SAA "rtr reaction-configuration" command. **This option is not currently supported.**	Supported	Not supported
cartridge.cisco.saa.action.nmvt.isSupported	true	Cisco Support for SAA Threshold Action-Type Nmvt Indicates whether the 'nmvt' threshold action-type is supported for the SAA "rtr reaction-configuration" command. A fault is raised if this value is set to 'false' and the action type is set to 'nmvt'.	Supported	Not supported
cartridge.cisco.saa.rtr.reactionConfig.multipleMonitorElementsAllowed	false	Cisco SAA Rtr Reaction-Configuration Multiple Monitor Elements Allowed Indicates whether multiple monitor parameters are allowed for the SAA "rtr reaction-configuration" command. The monitor elements include the	Supported	Supported

Option	Default Value	Description	SM2DM	DM2CLI
		"connection-loss-enable", "timeout-enable", and "verify-error-enable" parameters. If the value is set to 'true', then multiple monitor elements are configured in a single "rtr reaction-configuration" command.		
cartridge.cisco.saa.jitter.maxInterval	0	Cisco SAA Jitter Operation Maximum Interval Value Indicates the maximum allowable Jitter interval value. The Jitter interval value is calculated by multiplying the number of packets by the inter-packet interval. A value of 0 means that there is no maximum on the device A fault is raised if the Jitter interval is greater than the specified value.	Supported	Not supported
cartridge.cisco.saa. removeProbeTwice	false	Cisco SAA RTR Probe to be Removed Twice Indicates whether to send the "no rtr {probe-id}" command twice in order to remove the RTR Probe. If the value is set to 'true', then the "no rtr {probe-id}" command is sent twice whenever it is used.	Not supported	Supported
cartridge.cisco.saa.rtr.thresholdType.average.isSupported	true	Cisco Support for SAA Threshold-Type Average Indicates whether the "threshold-type average" parameter is supported for the SAA "rtr reaction-configuration" command. A fault is raised if this	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		value is set to 'false' and the threshold type is set to 'average'.		
cartridge.cisco.saa.rtr.thresholdType.consecutive.isSupported	true	Cisco Support for SAA Threshold-Type Consecutive Indicates whether the "threshold-type consecutive" parameter is supported for the SAA "rtr reaction-configuration" command. A fault is raised if this value is set to 'false' and the threshold type is set to 'consecutive'.	Supported	Not supported
cartridge.cisco.saa.rtr.commandSyntax	rtr	Cisco SAA RTR Command Syntax Indicates which command syntax to use when provisioning SAA RTR configurations. Changing this value will change the command syntax for all future SAA RTR configurations.	Supported	Supported
cartridge.cisco.saa.icmpEcho.commandSyntax	type echo protocol ipIcmpEcho	Cisco SAA Icmp Echo Command Syntax Indicates which command syntax to use when provisioning SAA Icmp Echo configurations. Changing this value will change the command syntax for all future SAA Icmp Echo operations.	Not supported	Supported
cartridge.cisco.saa.udpEcho.commandSyntax	type udpEcho	Cisco SAA UDP Echo Command Syntax	Not supported	Supported

Option	Default Value	Description	SM2DM	DM2CLI
		Indicates which command syntax to use when provisioning SAA UDP Echo configurations. Changing this value will change the command syntax for all future SAA UDP Echo operations.		
cartridge.cisco.saa.tcpConnect.commandSyntax	type tcpConnect	Cisco SAA TCP Connect Command Syntax Indicates which command syntax to use when provisioning SAA TCP Connect configurations. Changing this value will change the command syntax for all future SAA TCP Connect operations.	Not supported	Supported
cartridge.cisco.saa.jitter.commandSyntax	type jitter	Cisco SAA Jitter Command Syntax Indicates which command syntax to use when provisioning SAA Jitter configurations. Changing this value will change the command syntax for all future SAA Jitter operations.	Not supported	Supported
cartridge.cisco.saa.bucketOfHistoryKept.commandSyntax	buckets-of-history-kept	Cisco SAA History-Buckets Command Syntax Indicates which command syntax to use when provisioning SAA History-Buckets configurations. Changing this value will change the command syntax for all future SAA History-Buckets operations.	Not supported	Supported

Option	Default Value	Description	SM2DM	DM2CLI
cartridge.cisco.saa.filterForHistory.commandSyntax	filter-for-history	Cisco SAA History-Filter Command Syntax Indicates which command syntax to use when provisioning SAA History-Filter configurations. Changing this value will change the command syntax for all future SAA History-Filter operations.	Not supported	Supported
cartridge.cisco.saa. livesOfHistoryKept.commandSyntax	lives-of-history-kept	Cisco SAA History-Lives-Kept Command Syntax Indicates which command syntax to use when provisioning SAA History-Lives-Kept configurations. Changing this value will change the command syntax for all future SAA History-Lives-Kept operations.	Not supported	Supported
cartridge.cisco.saa.icmpEcho. requestDataSize.minimum	0	Cisco SAA ICMP Echo Request-Data-Size Minimum Value Indicates the minimum allowable value for the "request-data-size" command in SAA ICMP Echo operations. A fault is raised if the request size is less than the specified value.	Supported	Not supported
cartridge.cisco.saa.icmpEcho. requestDataSize.maximum	65535	Cisco SAA ICMP Echo Request-Data-Size Maximum Value Indicates the maximum allowable value for the "request-data-size" command in SAA ICMP Echo operations.	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		A fault is raised if the request size is greater than the specified value.		
cartridge.cisco.saa.udpEcho.requestDataSize.minimum	4	Cisco SAA UDP Echo Request-Data-Size Minimum Value Indicates the minimum allowable value for the "request-data-size" command in SAA UDP Echo operations. A fault is raised if the request size is less than the specified value.	Supported	Not supported
cartridge.cisco.saa.udpEcho.requestDataSize.maximum	8192	Cisco SAA UDP Echo Request-Data-Size Maximum value Indicates the maximum allowable value for the "request-data-size" command in SAA UDP Echo operations. A fault is raised if the request size is greater than the specified value.	Supported	Not supported
cartridge.cisco.saa.tcpConnect.requestDataSize.minimum	0	Cisco SAA TCP Connect Request-Data-Size Minimum Value Indicates the minimum allowable value for the "request-data-size" command in SAA TCP Connect operations. A fault is raised if the request size is less than the specified value.	Supported	Not supported
cartridge.cisco.saa.tcpConnect.requestDataSize.maximum	65535	Cisco SAA TCP Connect Request-Data-Size Maximum Value	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		Indicates the maximum allowable value for the "request-data-size" command in SAA TCP Connect operations. A fault is raised if the request size is greater than the specified value.		
cartridge.cisco.saa.icmpEcho.frequency.minimum	0	Cisco SAA ICMP Echo Frequency Minimum Value Indicates the minimum allowable frequency value for SAA ICMP Echo operations. A fault is raised if the period setting is less than the specified value.	Supported	Not supported
cartridge.cisco.saa.icmpEcho.frequency.maximum	604800	Cisco SAA ICMP Echo Frequency Maximum Value Indicates the maximum allowable frequency value for SAA ICMP Echo operations. A fault is raised if the period setting is greater than the specified value.	Supported	Not supported
cartridge.cisco.saa.udpEcho.frequency.minimum	0	Cisco SAA UDP Echo Frequency Minimum Value Indicates the minimum allowable frequency value for SAA UDP Echo operations. A fault is raised if the period setting is less than the specified value.	Supported	Not supported
cartridge.cisco.saa.udpEcho.frequency.maximum	604800	Cisco SAA UDP Echo Frequency Maximum Value	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		Indicates the maximum allowable frequency value for SAA UDP Echo operations. A fault is raised if the period setting is greater than the specified value.		
cartridge.cisco.saa.tcpConnect.frequency.minimum	0	Cisco SAA TCP Connect Frequency Minimum Value Indicates the minimum allowable frequency value for SAA TCP Connect operations. A fault is raised if the period setting is less than the specified value.	Supported	Not supported
cartridge.cisco.saa.tcpConnect.frequency.maximum	604800	Cisco SAA TCP Connect Frequency Maximum Value Indicates the maximum allowable frequency value for SAA TCP Connect operations. A fault is raised if the period setting is greater than the specified value.	Supported	Not supported
cartridge.cisco.saa.jitter.frequency.minimum	0	Cisco SAA Jitter Frequency Minimum Value Indicates the minimum allowable frequency value for SAA Jitter operations. A fault is raised if the period setting is less than the specified value.	Supported	Not supported
cartridge.cisco.saa.jitter.frequency.maximum	604800	Cisco SAA Jitter Frequency Maximum Value Indicates the maximum	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		allowable frequency value for SAA Jitter operations. A fault is raised if the period setting is greater than the specified value.		
cartridge.cisco.saa.timeout.minimum	0	Cisco SAA Timeout Minimum Value Indicates the minimum allowable timeout value for SAA operations. A fault is raised if the timeout setting is less than the specified value.	Supported	Not supported
cartridge.cisco.saa.timeout.maximum	604800000	Cisco SAA Timeout Maximum Value Indicates the maximum allowable timeout value for SAA operations. A fault is raised if the timeout setting is greater than the specified value.	Supported	Not supported
cartridge.cisco.saa.liveOfHistoryKept.minimum	0	Cisco SAA History-Lives-Kept Minimum Value Indicates the minimum allowable "History Lives Kept" value for SAA operations. A fault is raised if the lives kept setting is less than the specified value.	Supported	Not supported
cartridge.cisco.saa.liveOfHistoryKept.maximum	2	Cisco SAA History-Lives-Kept Maximum Value Indicates the maximum allowable "History Lives Kept" value for SAA operations. A fault is raised if the lives kept setting is greater than the specified value.	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
cartridge.cisco.saa. bucketsOfHistoryKept.minimum	1	Cisco SAA History-Buckets Minimum Value Indicates the minimum allowable "History Buckets" value for SAA operations. A fault is raised if the history bucket setting is less than the specified value.	Supported	Not supported
cartridge.cisco.saa. bucketsOfHistoryKept.maximum	60	Cisco SAA History-Buckets Maximum Value Indicates the maximum allowable "History Buckets" value for SAA operations. A fault is raised if the history bucket setting is greater than the specified value.	Supported	Not supported
cartridge.cisco.saa.jitter. numOfPackets.minimum	1	Cisco SAA Jitter Num-Packets Minimum Value Indicates the minimum allowable number of packets value for SAA Jitter operations. A fault is raised if the "Packets in sequence" setting is less than the specified value.	Supported	Not supported
cartridge.cisco.saa.jitter. numOfPackets.maximum	60000	Cisco SAA Jitter Num-Packets Maximum Value Indicates the maximum allowable number of packets value for SAA Jitter operations. A fault is raised if the "Packets in sequence"	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		setting is greater than the specified value.		
cartridge.cisco.saa.jitter.InterpacketInterval.minimum	1	Cisco SAA Jitter Interpacket-Interval Minimum Value Indicates the minimum allowable interpacket interval value for SAA Jitter operations. A fault is raised if the interpacket interval setting is less than the specified value.	Supported	Not supported
cartridge.cisco.saa.jitter.InterpacketInterval.maximum	60000	Cisco SAA Jitter Interpacket-interval Maximum Value Indicates the maximum allowable interpacket interval value for SAA Jitter operations. A fault is raised if the interpacket interval setting is greater than the specified value.	Supported	Not supported
cartridge.cisco.saa.tos.hexaDecimalValue	false	Cisco SAA Send TOS Value in Hexadecimal Indicates whether the TOS value should be sent in hexadecimal format. If the value is set to 'true', the TOS value is sent in hexadecimal format. If the value is set to 'false', the TOS value is sent in decimal format.	Not supported	Supported
cartridge.cisco.saa.actionType.Nmvt.isDefault	false	Cisco SAA Threshold Action-Type Nmvt Is Default	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		Indicates whether the device uses the 'nmvt' action-type by default for the SAA "rtr reaction-configuration" command. If the value is set to 'true', the 'nmvt' action-type parameter is not sent when issuing the "rtr reaction-configuration" command.		
cartridge.cisco.saa.requestDataSize.configureDefault	false	Cisco SAA Request Data Size Configure Default Indicates whether the "request-data-size" command should be issued for SAA operations when the request size is set to 'Default'. true - the command is issued when the request size is set to 'Default' false - the command is not issued when the request size is set to 'Default' The following request sizes are used when the value is set to 'true': TCP Connect - 1 UDP Echo - 16 ICMP Echo - 28 Jitter - 32	Supported	Not supported
cartridge.cisco.saa.thresholdFalling.configureDefault	false	Cisco SAA Threshold Falling Configure Default Indicates whether the "threshold-falling" parameter should be issued for SAA operations when the Threshold Falling	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		value is set to 'Default'. If this option is set to 'true', the "threshold-falling" value is set to 5000 milliseconds. If this option is set to 'false', the "threshold-falling" parameter is not configured.		
cartridge.cisco.saa.reactionConfig.isOldSyntaxSupported	false	Cisco SAA Support for Old Syntax for Reaction Configuration Indicates whether the device supports the old syntax for the SAA "reaction-configuration" command. A fault is raised if this value is set 'false' and an attempt is made to use the old syntax via the "cartridge.cisco.saa.reactionConfig.useOldSyntax" option.	Supported	Not supported
cartridge.cisco.saa.reactionConfig.useOldSyntax	false	Cisco SAA Use the Old Syntax for Reaction Configuration Indicates whether the old syntax should be used when issuing the "reaction-configuration" command for SAA operations. If the value is set to 'true', the old syntax is used for the "reaction-configuration" command.	Supported	Supported
cartridge.cisco.netflow.secondaryIpPort.isSupported	true	Cisco Support for NetFlow Secondary Destination IP Address and Port	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		Indicates whether a secondary destination IP address and port can be set for NetFlow configurations. A fault is raised if this value is set to 'false' and an attempt is made to configure a secondary IP address.		
cartridge.cisco.netflow.samplingModePacketInterval.isConfigured	false	Cisco NetFlow Cache Sampling Mode Configuration Indicates whether the sampling mode should be configured on the device for NetFlow configurations. If this value is set to 'true', the following command is issued as part of the NetFlow configuration: ip flow-sampling-mode packet-interval 10	Supported	Not supported
cartridge.cisco.netflow.mainCache.cacheEntriesConfiguration.isSupported	true	Cisco Support for NetFlow Version Cache Size Indicates whether the device supports cache entries for NetFlow configurations. A fault is raised if this value is set to 'false' and the cache value is greater than zero.	Supported	Not supported
cartridge.cisco.netflow.routeCacheSampled.isConfigured	false	Cisco NetFlow Cache Sampled Mode Configuration Indicates whether Sampled NetFlow should be enabled on the interface. If the value is set to 'true',	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		the Sampled NetFlow is enabled via the 'sampled' parameter: ip route-cache flow sampled If the value is set to 'false', the normal NetFlow is enabled as follows: ip route-cache flow		
cartridge.cisco.netflow.inactiveTimeout.immediately.isSupported	false	Cisco Support for NetFlow Inactive timeout Immediately Indicates whether inactive flow timeout immedialtely is supported.	Supported	Not supported
cartridge.cisco.ppp.multilink.fragment.useDisableFlag	false	Cisco Support for PPP Multilink Fragment Disable Indicates if "ppp multilink fragment disable" needs to be sent instead of "no ppp multilink fragmentation" Changing this value alters the command used to disable ppp multilink fragmentation on the router.	Not supported	Supported
cartridge.cisco.qos.policymap.policeWithMplsAction	SetMplsExp Transmit	Cisco Police MPLS Action Indicates which MPLS action to use in the police command when the marking value is less than 8: SetMplsExpTransmit (default) - the 'set-mpls-exp-transmit' parameter is used SetMplsExpImpositionTransmit -	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		the 'set-mpls-exp-imposition-transmit' parameter is used		
cartridge.cisco.qos.interface.defaultWREDType	precedence	Cisco Default WRED Type for Interface Indicates which WRED type to use by default in interface configuration mode. dscp - the following command is issued: random-detect dscp-based precedence - the following command is issued: random-detect	Supported	Not supported
cartridge.cisco.vpn.vrf.vrfRoutePolicy.suppressExportRouteTargets	false	Cisco VRF Route Policy Export Route Target Suppression Indicates whether export route target suppression is enabled: true - suppression is enabled, so any route target values specified in the "VPN Target" field of associated VRF Route Policy configuration policies is suppressed (ie. the "route-target export" statement is not configured in the VRF for these route	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		targets) false - suppression is not enabled, so all export route targets will be added to the VRF		
cartridge.cisco.qos.classmap.useAclForMatchAny	false	Cisco Use IPv4 ACL Instead of Match Any in Class Map Indicates whether an ACL should be used instead of the "match any" statement in the class map for classification groups with the "Match Any" option selected: true - an ACL is referenced in the class map via the "match access-group" command: class-map match-any map-name match access-group name acl-name false - the "match any" statement is used in the class map: class-map match-any map-name match any This option is ignored when using strict aggregation, so the “match any” statement will be used in the class-map. This option only applies when the "Match Any" option is selected in the classification group.	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
cartridge.cisco.qos.classmap.useIPv6AclForMatchAny	false	Cisco Use IPv6 ACL Instead of Match Any in Class Map Indicates whether an ACL should be used instead of the "match any" statement in the class map for classification groups with the "Match Any" option selected: true - an ACL is referenced in the class map via the "match access-group" command: class-map match-any map-name match access-group name acl-name false - the "match any" statement is used in the class map: class-map match-any map-name match any This option is ignored when using strict aggregation, so the “match any” statement will be used in the class-map. This option only applies when the "Match Any" option is selected in the classification group.	Supported	Not supported
cartridge.cisco.interface.suppressNoIPv6Enable	false	Specifies whether 'no ipv6 enable' command should be issued or not when all the ipv6 addresses which are configured through IPSA are removed. true - 'no ipv6 enable' command will be suppressed and not		

Option	Default Value	Description	SM2DM	DM2CLI
		sent to the device. false - 'no ipv6 enable' command will be sent to the device. If this value is 'false', then remaining devices support flowcontrol either with send or receive command apart from 2900XL and 3500XL series switches		
cartridge.cisco.qos.policymap.queuelimit.lowLimit	1	Cisco QOS Congestion Avoidance Queue Limit Minimum Value Indicates the minimum allowable value for the congestion avoidance queue limit. A fault is raised if the queue limit is less than the specified value.	Supported	Not supported
cartridge.cisco.qos.policymap.queuelimit.highLimit	8192000	Cisco QOS Congestion Avoidance Queue Limit Maximum Value Indicates the maximum allowable value for the congestion avoidance queue limit. A fault is raised if the queue limit is greater than the specified value.	Supported	Not supported
cartridge.cisco.qos.policymap.llq.defaultCOS	true	Cisco LLQ Support for Default Class of Service Indicates whether the LLQ MQC action is supported when using the default class of service. A fault is raised if this value is set to 'false' and LLQ is selected as an action for the default class of service.	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
cartridge.cisco.qos.policymap.llq.defaultWFQ	false	Cisco LLQ Support for Default WFQ Indicates whether the LLQ and Default WFQ actions can both be selected in a single MQC PHB group. A fault is raised if this value is set to 'false' and both the LLQ and Default WFQ actions are selected.	Supported	Not supported
cartridge.cisco.qos.mapclass.fragment.lowLimit	16	Cisco FRTS FRF.12 Fragment Size Minimum Indicates the minimum allowable value for the FRTS FRF.12 fragment size. A fault is raised if the fragment size is less than the specified value.	Supported	Not supported
cartridge.cisco.qos.frts.concurrentPolicy	allTargets	Cisco FRTS Concurrent Policy Application Indicates whether an FRTS policy can be applied to different targets concurrently: allTargets (default) - the service policy can be applied to multiple targets subOrInterface - the service policy can not be applied to multiple targets A fault is raised if the value is set to 'subOrInterface' and an FRTS policy is concurrently applied on a main interface and one of its subinterfaces.	Not supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
cartridge.cisco.qos.policymap.congestion.allowedMqcAction	shapingCbwfq	Cisco Other MQC Actions Allowed with Congestion Indicates which other MQC actions are allowed in conjuction with congestion: shapingCbwfq (default) - shaping and CBWFQ are both allowed when congestion is selected cbwfq - only CBWFQ is allowed when congestion is selected A fault is raised if the value is set to 'cbwfq' and the Congestion, CBWFQ, and Shape actions are all selected on an MQC PHB group.	Supported	Not supported
cartridge.cisco.qos.interface.frtsCommand	true	Cisco Support for the Frame-Relay Traffic-Shaping Command Indicates whether the device supports the "frame-relay traffic-shaping" command on Frame Relay interfaces: true - the "frame-relay traffic-shaping" command is issued false - the "frame-relay traffic-shaping" command is not issued	Not supported	Supported
cartridge.cisco.qos.policymap.shaping.basic	true	Cisco Support for Default Shaping Indicates whether the device supports default shaping for MQC PHB	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		groups. A fault is raised if this value is set to 'false' and default shaping is selected.		
cartridge.cisco.qos.policymap.shaping.peak	true	Cisco Support for Peak Shaping Indicates whether the device supports peak shaping for MQC PHB groups. A fault is raised if this value is set to 'false' and peak shaping is selected.	Supported	Not supported
cartridge.cisco.qos.policymap.shaping.average	true	Cisco Support for Average Shaping Indicates whether the device supports average shaping for MQC PHB groups. A fault is raised if this value is set to 'false' and average shaping is selected.	Supported	Not supported
cartridge.cisco.qos.policymap.shaping.maxbuffers	true	Cisco Support for Shaping Buffers Indicates whether the device supports the shaping buffers setting for MQC PHB groups. A fault is raised if this value is set to 'false' and the shaping buffers value is greater than zero.	Supported	Not supported
cartridge.cisco.qos.mapclass.supportsFrtsHoldQDepth	true	Cisco Support for FRTS Hold Queue Depth Indicates whether the device supports the FRTS	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		"frame-relay holdq" command. A fault is raised if this value is set to 'false' and the FRTS hold queue depth is greater than zero.		
cartridge.cisco.qos.mapclass.deployOnInterface	false	Cisco Support for FRF command on interface Indicates if the frame-relay fragmentation should be applied directly to the interface or put in the mapClass. This option should only be used on routers supporting the “frame-relay fragment” command under the interface context.	Supported	Not supported
cartridge.cisco.qos.interface.supportsAtmHoldQDepth	true	Cisco Support for ATM Hold Queue Depth Indicates whether the device supports the ATM "vc-hold-queue" command. A fault is raised if this value is set to 'false' and the ATM hold queue depth is greater than zero.	Supported	Not supported
cartridge.cisco.vlan.isSwitchportCommandSupported	true	Cisco Support for the Switchport Command Indicates whether the device supports the "switchport" command for placing an interface into Layer 2 mode. true - the "switchport" command is used false - the "switchport mode" command is used	Not supported	Supported

Option	Default Value	Description	SM2DM	DM2CLI
cartridge.cisco.vlan.isNonegotiateSupported	true	Cisco Support for the Switchport No Negotiate Command Indicates whether the device supports the "switchport nonegotiate" command. A fault is raised if this value is set to 'false' and the No Negotiate value is set for a VLAN interface.	Supported	Supported
cartridge.cisco.vlan.isQinqSupported	true	Cisco Support for 802.1Q Traffic Indicates whether the device supports the "dot1q-tunnel" parameter for the "switchport mode" command. A fault is raised if this value is set to 'false' and the qinq VLAN ID is set for a VLAN interface.	Supported	Not supported
cartridge.cisco.vlan.defaultEncapsulation	true	Cisco Default Switchport Trunk Encapsulation Indicates whether the default encapsulation should be restored when removing the trunk encapsulation. true - the following command is issued when removing encapsulation: default switchport trunk encapsulation false - the following command is issued when removing the encapsulation: no switchport trunk encapsulation	Not supported	Supported

Option	Default Value	Description	SM2DM	DM2CLI
cartridge.cisco.vlan.allowAdditionalVlanIds	false	Cisco Configure Additional VLAN IDs Indicates whether VLAN IDs 1 and 1002-1005 should be configured in addition to the IDs specified in the VLAN Interface configuration policy for tagged VLANs. true - VLAN IDs 1 and 1002-1005 are configured in addition to the values you specify false - only the VLAN ID values you specify are configured	Supported	Not supported
cartridge.cisco.vlan.accessVlanId.minimum	1	Cisco Untagged VLAN ID Minimum Value Indicates the minimum allowable VLAN ID value for untagged VLANs. A fault is raised if the VLAN ID is less than the specified value.	Supported	Not supported
cartridge.cisco.vlan.accessVlanId.maximum	4094	Cisco Untagged VLAN ID Maximum Value Indicates the maximum allowable VLAN ID value for untagged VLANs. A fault is raised if the VLAN ID is greater than the specified value.	Supported	Not supported
cartridge.cisco.vlan.allowedVlanId.minimum	1	Cisco Tagged VLAN ID Minimum Value Indicates the minimum allowable VLAN ID value for tagged VLANs. A fault is raised if the	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		VLAN ID is less than the specified value.		
cartridge.cisco.vlan.allowedVlanId.maximum	4094	Cisco Tagged VLAN ID Maximum Value Indicates the maximum allowable VLAN ID value for tagged VLANs. A fault is raised if the VLAN ID is greater than the specified value.	Supported	Not supported
cartridge.cisco.vlan.vlanIds.isDuplicateAllowed	true	Cisco Tagged VLAN IDs Validation on Duplicates Indicates if the vlan id duplication in VLAN IDs is allowed for tagged VLANs. A fault is raised if the application is not allowed when duplication happens.	Supported	Not supported
cartridge.cisco.vlan.mgmtVlanInterface.validate	false	Cisco Management VLAN Interface Validation on missing Indicates if validation is needed for missing mgmtVlanInterface. A fault is raised if the mgmtVlanInterface is missing when this option is set to true.	Supported	Not supported
cartridge.cisco.vlan.vlanDefinition.isReduced	false	Cisco VLAN Definition Reduction Indicates if vlan reduction is needed for the vlanDefinition. A fault is raised if this option is 'false' and there are duplicate vlan ids on one interface.	Supported	Not supported
cartridge.cisco.vlan.mtu.minimum	576	Cisco VLAN MTU Minimum Value	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		Indicates the minimum allowable VLAN MTU value. A fault is raised if the MTU value is less than the specified value.		
cartridge.cisco.vlan.mtu.maximum	18190	Cisco VLAN MTU Maximum Value Indicates the maximum allowable VLAN MTU value. A fault is raised if the MTU value is greater than the specified value.	Supported	Not supported
cartridge.cisco.vlan.commandSyntax	vlan	Cisco VLAN Command Syntax Indicates whether VLANs are provisioned in global configuration mode or in VLAN configuration mode. vlan - provisioning is done in global configuration mode via the "conf t" command vlan database - provisioning is done in VLAN configuration mode via the "vlan database" command	Supported	Supported
cartridge.cisco.vlan.audit.adjacentVlanIdsSeparator	comma	Cisco Consecutive VLAN IDs Separator Indicates which separator to use when configuring two consecutive VLAN IDs. comma - the IDs are separated by a comma: vlan 3,4 hyphen - the IDs are	Not supported	Supported

Option	Default Value	Description	SM2DM	DM2CLI
		separated by a hyphen: vlan 3-4 This value should be set according to the format displayed by the device so that audits can compare the values correctly. This option is only used when provisioning VLANs in global configuration mode. It is ignored if VLAN configuration mode is being used. For more information, see the description of the option: "cartridge.cisco.vlan.commandSyntax"		
cartridge.cisco.vlan.portChars.flowControlSend.isSupported	true	Cisco Support for the Flow Control Send Command Indicates whether the device supports the "flowcontrol send" command in interface configuration mode. This command is used when configuring an interface to send pause frames. A fault is raised if this value is set to 'false' and the Flow Control Send value is set in the Cisco Ethernet Port Characteristics configuration policy.	Supported	Not supported
cartridge.cisco.vlan.portChars.flowControl.isSupported	true	Cisco Support for the Flow Control Command Indicates whether the device supports the "flowcontrol" command in interface configuration mode.	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		A fault is raised if this value is set to 'false' and any Flow Control values are set in the Cisco Ethernet Port Characteristics configuration policy.		
cartridge.cisco.vlan.portChars.xlflowControl.isSupported	false	Cisco 2900XL and 3500XL series switches support flowcontrol symmetric and asymmetric Indicates flowcontrol or flowcontrol asymmetric or flowcontrol symmetric command is accepted on this XL series switches. If this value is 'true', then these XL series switches support flowcontrol with symmetric or asymmetric command. If this value is 'false', then remaining devices support flowcontrol either with send or receive command apart from 2900XL and 3500XL series switches.	Supported	Not supported
cartridge.cisco.vlan.portChars.portStormControl.isSupported	true	Cisco Support for the Storm Control Command Indicates whether the device supports the "storm-control" command in interface configuration mode. A fault is raised if this value is set to 'false' and the 3500 Storm Control values are set in the Cisco Ethernet Port Characteristics configuration policy.	Supported	Not supported
cartridge.cisco.vlan.portChars.mlsQosTrustType.isSupported	true	Cisco Support for the Mls Qos Trust Command	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		Indicates whether the device supports the "mls qos trust" command in interface configuration mode. A fault is raised if this value is set to 'false' and the Trust Type value is set in the Cisco Ethernet Port Characteristics configuration policy.		
cartridge.cisco.vlan.portChars.stormControlThreshold.isSupported	true	Cisco Support for Storm Control Threshold Indicates whether the device supports the "storm-control" command in interface configuration mode. A fault is raised if this value is set to 'false' and the Storm Control threshold is set in the Cisco Ethernet Port Characteristics configuration policy.	Supported	Not supported
cartridge.cisco.vlan.portChars.isDuplexDependentOnSpeed	true	Cisco Dependency Between Duplex and Speed Indicates whether the configuration of the "duplex" command is dependent on the "speed" command being issued beforehand. If this value is set to 'true', then the Speed value in the Cisco Ethernet Port Characteristics configuration policy must be set to any value besides 'auto' whenever a Duplex value is set. Otherwise, a fault is	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		raised.		
cartridge.cisco.vlan.portChars.spanningTreeRootGuard.isOldSyntaxSupported	false	Cisco Support for the Old Syntax of the Spanning Tree Guard Configuration Indicates whether the configuration of the spanning-tree guard mode should be done using the old syntax: true - the old syntax is used: spanning-tree <*mode*> guard false - the new syntax is used: spanning-tree guard <*mode*>	Not supported	Supported
cartridge.cisco.vlan.portChars.udldEnable	false	Cisco XL series switches support udld enable Indicates udld port aggressive command is accepted as udld enable on this XL series switches. If this value is 'true', then XL series switches support udld enable command. If this value is 'false', then remaining devices support udld port aggressive command apart from XL series switches.	Not supported	Supported
cartridge.cisco.vlan.portChars.srrQueueBandwidthShape.isSupported	false	Cisco srr-queue bandwidth shape Indicates that through ciscoEthernetPortCharacteristics policy srr-queue bandwidth shape command is supported [through SRR queue bandwidth shape] only for Cisco 3750G and Cisco 3750ME switches.	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		The srr-queue bandwidth shape commands will be generated only if the value is true.		
cartridge.cisco.vlan.portChars.mdixAuto.isSupported	false	Cisco MDIX-Auto Indicates that through ciscoEthernetPortCharacteristics policy mdix auto command is supported [through Auto-MDIX] only for Cisco 3750G switch. The mdix auto commands will be generated only if the value is true.	Supported	Not Supported
cartridge.cisco.vlan.portChars.speed.nonegotiate.isSupported	true	Cisco Speed Nonegotiate Support Indicates that through ciscoEthernetPortCharacteristics policy speed nonegotiate is supported [through Port Negotiation (GBIC only)] for all devices, except for Cisco 3508G XL and 3512XL with IOS (12.0(5)WC9a). If this value is 'false', then the command will be sent as either "negotiation auto" or "no negotiation auto".	Not supported	Supported
cartridge.cisco.vlan.portChars.defaultSpeed.isSupported	True	Cisco Default Speed Support Indicates that through ciscoEthernetPortCharacteristics policy “default speed” is supported [through Port Negotiation (GBIC only)]. If this value is ‘false’, the command will be sent as “no speed nonegotiation”.		
cartridge.cisco.vlan.portChars.negotiation.isSupported	false	Cisco Negotiation Support Indicates that through ciscoEthernetPortCharacte	Not supported	Supported

Option	Default Value	Description	SM2DM	DM2CLI
		ristics policy negotiation command is supported [through Port Negotiation (GBIC only)] only for Cisco 3508G XL and 3512XL with IOS (12.0(5)WC9a). If this value is 'true', then the command will be sent as either "negotiation auto" or "no negotiation auto".		
cartridge.cisco.vpn.ospf.spfthrottle.commandSyntax	timers throttle spf	Cisco VPN OSPF SPF Throttling Command Syntax Indicates which command syntax to use when provisioning VPN OSPF SPF Throttling configurations. Changing this value will change the command syntax for all future VPN OSPF SPF Throttling configurations.	Not supported	Supported
cartridge.cisco.vpn.ospf.maximumPath.minimum	1	Cisco ospf maximum-path Minimum Value Defines the minimum value for the maximum-path. A fault is raised if the maximum-path is less than the specified value.	Supported	Not supported
cartridge.cisco.vpn.ospf.maximumPath.maximum	16	Cisco ospf maximum-path Maximum Value Defines the maximum value for the maximum-path. A fault is raised if the maximum-path is greater than the specified value.	Supported	Not supported
cartridge.cisco.controller.au4tug3.isSupported	true	Cisco StmlChannelizedSerialInterface Policy, controller au-4-tug-3 Support	Supported	Not supported

Option	Default Value	Description	SM2DM	DM2CLI
		Indicates that au-4-tug-3 command is not supported on 3500 and 3600 devices with IOS 12.0 (14) S and 12.2 (15) T. If this value is 'true', au-4-tug-3 command is supported.		
cartridge.cisco.interface. chooseDescFromWhenConflictOccurs	default	Cisco Method for Choosing the Interface Description Specifies which interface description to use when multiple conflicting descriptions are found: default - No conflict detection is performed. This means that the conflicting descriptions may overwrite each other. configPolicy - Use the value specified in the subinterface creation configuration policy. site - Use the value specified in the VPN site.	Supported	Not supported
cartridge.cisco.interface.suppressNoIPv6Enable	false	Suppress removal of IPv6 enablement on an Interface Specifies whether 'no ipv6 enable' command should be issued or not when all the ipv6 addresses which are configured through IP Service Activator are removed. false – 'no ipv6 enable' command will be sent to the device. true – 'no ipv6 enable' command will be suppressed and not	Not supported	Supported

Option	Default Value	Description	SM2DM	DM2CLI
		sent to the device.		