Test Results Summary for IOS XE SD-WAN for Japan (Release Version 20.7.1/17.7.1)

First Published: 2022-06-07

Last Modified: 2022-06-13

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Overview

Cisco IOS XE SD-WAN

Cisco SD-WAN IOX SE test , an integral part of the enterprise solution, is a program that validates various Cisco IOS XE SD-WAN devices. This is achieved by testing the latest versions of Cisco IOS XE SD-WAN devices.

Cisco IOS XE SD-WAN devices for Japan , in turn is an add-on testing at the solution level, where the requirements gathered are specific to Japanese usage and market.

The requirements are derived based on the following:

- New features in SDWAN 20.7.1 - IOS XE 17.7.1
- High priority scenarios and basic regression features

The test execution is carried out on selected Cisco IOS XE SD-WAN devices, which affect the Japanese segment that are prioritized by Cisco Japan team.

The following Products and Applications are covered in the test execution:

- Cisco vManage,vBond,vSmart
- Cisco ESXi Host
- Cisco ISR C111X-8P
- Cisco ISR 4351
- Cisco ISR 4331
- Cisco ISR 1100
- Cisco Catalyst 8300
- Cisco Catalyst 8200
- Cisco Catalyst 8500
- Cisco Catalyst 8KV
- Cisco ISR4461
- Cisco ISR 4321
- Cisco Catalyst 9K PoE Switch

Acronyms

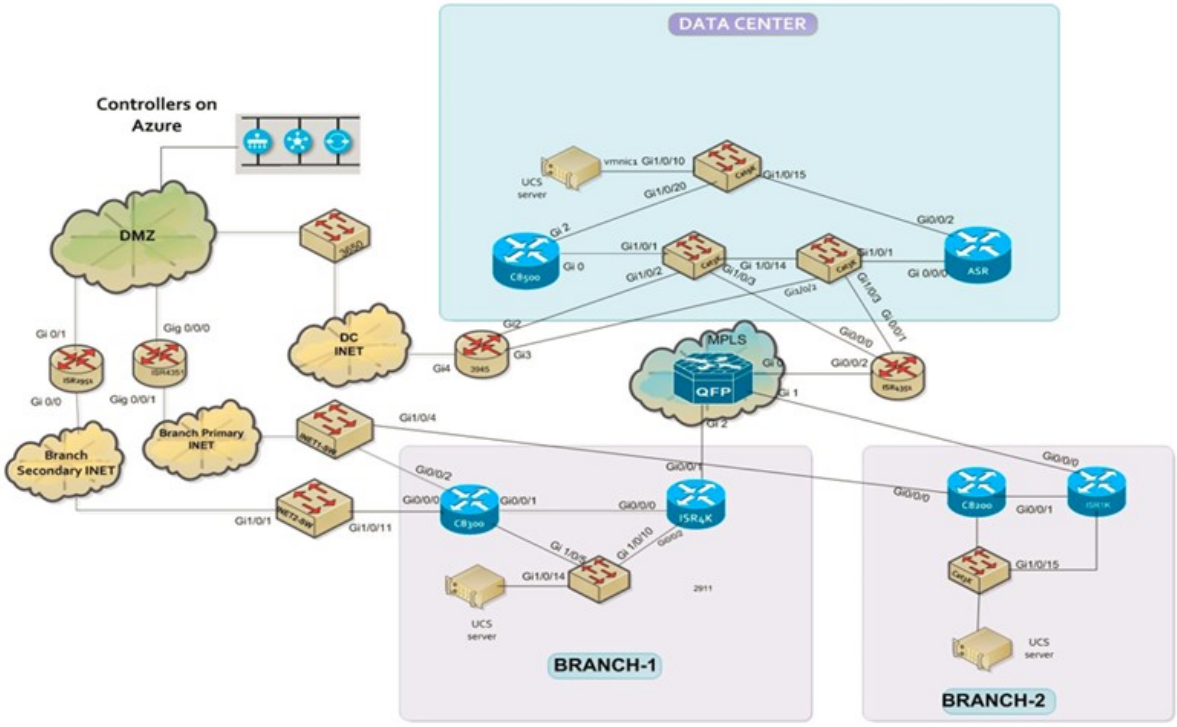
Acronym	Description
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AF	Address-family
API	Application Programming Interface
ASN	Autonomous System Number

ASR	Aggregation Services Routers
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BR	Branch
BR Site	Branch Site
CA	Certificate Authority
CDF	Cloud Delivered Firewall
cEdge Router	Cisco Edge Router
Cisco DNA	Cisco Digital Network Architecture
Config	Configuration
Config-t	Configuration-transaction
COM Port	Communication Port
CoR	Cloud on Ramp
CLI	Command Line
CSP	Cisco Cloud Services Platform
DC	Data Center
DHCP	Dynamic Host Configuration Protocol
DIA	Direct Internet Access
DNS	Domain Name System
DR	Disaster Recovery
DSCP	Differentiated Services Code Point
Dst	Destination
DTLS	Datagram Transport Layer Security
EF	Expedited Forwarding
EIGRP	Enhanced Interior Gateway Routing Protocol
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
FW	Firewall
Geo	Graphical
GUI	Graphical User Interface
GW Site	Gate Way Site
GRE	Generic Routing Encapsulation
HA	High Availability

HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IMIX	Internet Mix
Int	Interface
INET	Internet
IOS	Internetworking Operating System
IPS	Intrusion prevention system
ISR	Integrated Services Routers
LAN	Local Area Network
L3	Layer 3
L4	Layer 4
L7	Layer 7
MAN	Metropolitan Area Network
MPLS	Multi-Protocol Label Switching
MSG	Message
MTU	Maximum transmission unit
NA	Not Applicable
NAT	Network Address Translation
NTP	Network Time Protocol
NIC	Network Interface Card
OMP	Overlay Management Protocol
OSPF	Open Shortest Path First
O365	Office 365
PAT	Port Address Translation
PnP	Plug and Play

Test topology and Environment Matrix

Test Topology



Component Matrix

Applications	Component		Version
Controller Network	vManage	Version	20.7.1
	vBond	Version	20.7.1
	vSmart	Version	20.7.1
Communications Infrastructure	ISR C111X-8P	IOS XE SDWAN	17.7.1
	ISR 4351, 4331	IOS XE	17.7.1
	ISR 1100, Cat 8300, C8200 & C8500	IOS XE	17.7.1
	CAT 8KV	IOS XE	17.7.1
	ISR4461	IOS XE	17.7.1
	ASR 1002-X	IOS XE SDWAN	17.7.1
	ISR 4321	IOS XE SDWAN	17.7.1
	Cat 9K PoE Switch	Version	17.2
UCS	ESXi Host	UCSC-C240-M5SX	ESXi 6.0, 6.5
Client	Operating System	Windows 10	Windows 10
		Mozilla	95.0.1
		Chrome	96.0.4606.212

What's New ?

SDWAN 20.7.1 - IOS XE 17.7.1 Solution testing

- Support for HSRP and HSRP Authentication on Cisco IOS XE SD-WAN Devices
- Extended Visibility with Cisco SD-WAN and Cisco Thousand-Eyes - Cat8K
- GRE Over IPsec Tunnels Between Cisco IOS XE Devices
- UX 2.0 Monitoring
- TCP-UDP port tracker for static route
- Intra-VPN Service-side NAT
- SNMPv3 AES 256 - cedge Platforms
- Flexible Netflow for VPN0 Interface
- Granular Role-Based Access Control for Feature Templates
- RIPv2 support on Cisco IOS XE SD-WAN Devices

Open Caveats

Defect ID	Title
CSCwb22631	While creating SNMP user in ISR1100/CAT8k device CLI throws error
CSCwb61835	Wrong error validation is showing for Threshold value in CLI of 17.7
CSCwb61935	While configure the combination of tracker and DNS-name its throws the Error CLI of 17.7
CSCwb62150	Able to configure Access value as morethan boundary values CLI of 17.7
CSCwb67444	SNMPv3 command Release Notes needs to be modified as per CLI for IOX SE 17.7
CSCwb53554	Thousand Eye hostname is not reflecting in Docker details after changing the hostname
CSCwb55473	Token and Default hostname is not displaying up after installing the ThousandEye Agent
CSCwb65614	Unable to delete/readd the thousand eye profile in IOS XE of 17.7
CSCwb65635	Unable to change the CPU/Memory resource for Thousand Eye agent in IOS XE of 17.7
CSCwb55712	HSRP - No standby 100 preempt cmd is not working properly in in IOS XE of 17.7
CSCwb65457	HSRP - standy mac refresh interval command is not workiing in IOS XE of 17.7
CSCwb23903	Database memory leak issue detected in ISR4461/K9 platform
CSCwb63989	CLI template button is visible without CLI template read and write access in Vmanage dashboard
CSCwb64202	Default credentials not configured for netadmin user but warning displayed in vManage dashboard
CSCwb65298	vManage allowing netadmin user to delete itself, retain session and allow limited access
CSCwb65489	vManage Policy Access List Definition Builder API returning incorrect return error
CSCwb65829	Unable to change the ip mtu size as per the reference value in CLI for IOS XE17.7.1

New Features

Support for HSRP and HSRP Authentication on Cisco IOS XE SD-WAN Devices

Logical ID	Title	Description	Status	Defect ID
ENJ.HSRP.20.7.1.N.001	Enable & activate HSRP & Change the version of HSRP to HSRPv2.	Check HSRP is configurable and HSRPv2 is supported. Then verify HSPRv2 uses 224.0.0.102 multicast for sending hello packets.	Passed	
ENJ.HSRP.20.7.1.N.002	Configure HSRP priority and check higher priority is preferred.	Configure the same HSRP priority on R1 and R2(with lower <ip-address>) then configure a higher HSRP priority on R2 to check R2 becomes active.	Passed	
ENJ.HSRP.20.7.1.N.003	Configure HSRP priority. In case of same priority, higher IP device isn't elected when the interface is brought up after shutting down.	Configure the same HSRP priority on R1 and R2(with lower <ip-address>) then shut down R1 interface and bring it up after 12 seconds to check R2 is active.	Passed	
ENJ.HSRP.20.7.1.N.004	Configure & validate HSRP preemption on standby	With HSRP priority1 > priority2, configure priorty1 and priority2 on R1 and R2 respectively. Configure preempt on R1 and R2. Shut down R1 interface and bring it up and check R1 preempts after delay time.	Failed	CSCwb55712
ENJ.HSRP.20.7.1.N.005	Configure HSRP Authentication using MD5 and verify it's supported.	Configure HSRP Authentication using MD5 and verify it's supported. \u0007	Passed	

ENJ.HSRP.20.7.1.N.006	Configure HSRP hello & hold timers. Check when hello sent matches timer.	Check HSRP is configurable and HSRPv2 is supported. Then verify HSPRv2 uses 224.0.0.102 multicast for sending hello packets.	Passed	
ENJ.HSRP.20.7.1.N.007	Improve CPU & network performance with HSRP multiple group optimization and client group functionalities	Configure an HSRP group as a client group. Configure the HSRP client group refresh interval. Specify a virtual MAC address for HSRP. Configure the name of a standby group.	Failed	CSCwb65457
ENJ.HSRP.20.7.1.N.008	Configure HSRP using vManage CLI template	Configure HSRP using vManage Cli template \u0007	Passed	
ENJ.HSRP.20.7.1.N.009	Configure HSRP using active/standby - Failover	Configure HSRP on R1 and R2 then check <virtual-ip-address> is pingable. Shut down R1 interface and check <virtual-ip-address> is still pingable.	Passed	
ENJ.HSRP.20.7.1.N.010	Configure HSRP with multiple standby - Requirement 3 routers \u0007	Configure HSRP on 3 routers R1, R2 and R3 with priority1 > priority2 > priority3. \u0007	Passed	
ENJ.HSRP.20.7.1.N.011	Configure HSRP using active/active - loadbalancing \u0007	With HSRP priority1 > priority2, configure priorty1 and priority2 for group-number1 on R1 and R2 respectively. Configure priorty2 and priority1 for group-number2 on R1 and R2 respectively.	Passed	

ENJ.HSRP.20.7.1.N.012	Configure HSRP Authentication using text and verify it's supported.	Configure HSRP Authentication using text and verify it's supported.	Passed	
ENJ.HSRP.20.7.1.N.013	Static NAT with HSRP	Configure inside-local-interface. Configure outside-global-interface. Configure static NAT translation. \u0007	Passed	
ENJ.HSRP.20.7.1.N.014	Configure HSRP object tracking and verify it's supported.	Configure HSRP object tracking and verify it's supported.	Passed	
ENJ.HSRP.20.7.1.N.015	Configure HSRP object tracking and verify it's supported.	Configure HSRP object tracking and verify it's supported.	Passed	
ENJ.HSRP.20.7.1.N.016	Configure HSRP system tracking and verify it's supported.	Configure Static Route system tracking. Configure HSRP.	Passed	
ENJ.HSRP.20.7.1.N.017	Configure FHRP to Improve CPU & network performance	Configure Master and Client groups on R1 and R2. Verify Client group follows Master group.	Passed	
ENJ.HSRP.20.7.1.N.018	Configure & verify HSRP preemption is disabled	With HSRP, don't configure preempt. Check HSRP preemption is disabled.	Passed	
ENJ.HSRP.20.7.1.N.019	Configure & verify HSRP behavior without preemption	With HSRP priority1 > priority2, configure priorty1 and priority2 on R1 and R2 respectively. Don't configure preempt. Shut down R1 interface and bring it up and check R1 is still the active router after delay time.	Passed	

Intra-VPN Service-side NAT

Logical ID	Title	Description	Status	Defect ID
ENJ.ItraVpnSSN.20.7.1.N.001	Configure the static ip nat inside mapping with Natpool with VPN 100 in same site	Configure the static ip nat inside mapping with Natpool with VPN 100 in same site by using CLI	Passed	
ENJ.ItraVpnSSN.20.7.1.N.002	Configure the dynamic ip nat outside mapping Natpool with different site	Configured the dynamic ip nat outside mapping Nat pool with different site by using CLI	Passed	
ENJ.ItraVpnSSN.20.7.1.N.003	Configure the static nat of service side source ip address	Configure the static nat of service side ip address by using CLI	Passed	
ENJ.ItraVpnSSN.20.7.1.N.004	Configure the static inside nat and remove the pool to check the output	Configure the NATPool interface for VPN by using CLI	Passed	
ENJ.ItraVpnSSN.20.7.1.N.005	Configure the NAT Pool interface for VPN	Configure the static ip nat of outside mapping with natpool by using CLI	Passed	
ENJ.ItraVpnSSN.20.7.1.N.006	Configure the dynamic ip nat mapping with natpool	Configure the static ip nat of outside mapping with natpool by using CLI	Passed	
ENJ.ItraVpnSSN.20.7.1.N.007	Configure the Inside Dynamic & Dynamic Overload Service Side NAT	Configure the dynamic and overload by using data policy	Passed	
ENJ.ItraVpnSSN.20.7.1.N.008	Configure the outside Dynamic & Dynamic Overload Service Side NAT	Configure the outside dynamic and overload by using data policy	Passed	

ENJ.ItraVpnSSN.20.7.1.N.009	Configure the static ip nat with port forwarding in same site with physical interface	Configure the static ip nat with port forwarding in same site with physical interface by using data policy	Passed	
ENJ.ItraVpnSSN.20.7.1.N.010	Verify the Outside Dynamic with Inside static	Configure the outside dynamic with inside static by using data policy	Passed	
ENJ.ItraVpnSSN.20.7.1.N.011	Verify the Inside Dynamic with Outside static	Configure the Inside dynamic with Outside static by using data policy	Passed	
ENJ.ItraVpnSSN.20.7.1.N.012	Verify the outside Static & port forwarding Service Side NAT	Configure the outside static and port forwarding by using data policy	Passed	
ENJ.ItraVpnSSN.20.7.1.N.013	Configure the ip nat outside by using subinterface	Configure the ip nat outside for multiple subinterface by using CLI	Passed	
ENJ.ItraVpnSSN.20.7.1.N.014	Configure the intra VPN service side NAT with physical interface	Configure the intra VPN service side NAT with physical interface by using CLI	Passed	
ENJ.ItraVpnSSN.20.7.1.N.015	Configure static ip nat outside mapping with natpool and port forwarding	Configure the outside static and port forwarding with natpool by using CLI	Failed	CSCwb65829

Flexible Netflow for VPN0 Interface

Logical ID	Title	Description	Status	Defect ID
ENJ.FlexibleNetflow.20.7.1.N.001	Configure Flexible Netflow to monitor the traffic flow using cflowd collector	Configure Flexible Netflow & check the log Is collected in CFlow Collector	Passed	
ENJ.FlexibleNetflow.20.7.1.N.002	Configure Netflow to monitor the tunnel ingress(WAN > Cisco SD-WAN-tunnel > LAN) traffic by matching the dscp value	Configure Netflow to monitor the tunnel ingress(WAN > Cisco SD-WAN-tunnel > LAN) traffic by matching the dscp value	Passed	
ENJ.FlexibleNetflow.20.7.1.N.003	Configure Netflow to monitor the tunnel egress(LAN > Cisco SD-WAN-tunnel > WAN) traffic by matching the dscp value	Configure Netflow to monitor the tunnel egress(LAN > Cisco SD-WAN-tunnel > WAN) traffic by matching the dscp value	Passed	
ENJ.FlexibleNetflow.20.7.1.N.004	Configure Netflow to monitor the tunnel ingress traffic by matching the protocol udp	Configure Netflow to monitor the tunnel ingress traffic by matching the protocol udp	Passed	
ENJ.FlexibleNetflow.20.7.1.N.005	Configure Netflow to monitor the tunnel egress traffic by matching the protocol udp	Configure Netflow to monitor the tunnel egress traffic by matching the protocol udp	Passed	
ENJ.FlexibleNetflow.20.7.1.N.006	Configure Netflow to monitor the tunnel ingress traffic by matching the VPN 100	Configure Netflow to monitor the tunnel ingress traffic by matching the VPN 100	Passed	
ENJ.FlexibleNetflow.20.7.1.N.007	Configure Netflow to monitor the tunnel egress traffic by matching the VPN 200	Configure Netflow to monitor the tunnel egress traffic by matching the VPN 200	Passed	

ENJ.FlexibleNetflow.20.7.1.N.008	Configure Netflow to monitor the tunnel egress traffic by matching the VPN 200	Configure Netflow to monitor the tunnel ingress traffic by matching the port no	Passed	
ENJ.FlexibleNetflow.20.7.1.N.009	Configure Netflow to monitor the tunnel egress traffic by matching the port no	Configure Netflow to monitor the tunnel egress traffic by matching the port no	Passed	
ENJ.FlexibleNetflow.20.7.1.N.010	Configure Netflow to monitor the tunnel ingress traffic by matching the source interface	Configure Netflow to monitor the tunnel ingress traffic by matching the source interface	Passed	
ENJ.FlexibleNetflow.20.7.1.N.011	Configure Netflow to monitor the tunnel egress traffic by matching the source interface	Configure Netflow to monitor the tunnel egress traffic by matching the source interface	Passed	
ENJ.FlexibleNetflow.20.7.1.N.012	Configure Netflow to monitor the tunnels ingress using routing protocol ospf	Configure Netflow to monitor the tunnels ingress using routing protocol ospf	Passed	
ENJ.FlexibleNetflow.20.7.1.N.013	Configure Netflow to monitor the tunnels ingress using routing protocol ospf	Configure Netflow to monitor the tunnels ingress using routing protocol ospf	Passed	
ENJ.FlexibleNetflow.20.7.1.N.014	Configure netflow to monitor the tunnels ingress using routing protocol bgp	Configure Netflow to monitor the tunnels ingress using routing protocol bgp	Passed	
ENJ.FlexibleNetflow.20.7.1.N.015	Configure Netflow to monitor the tunnels egress using routing protocol ospf	Configure Netflow to monitor the tunnels egress using routing protocol ospf	Passed	
ENJ.FlexibleNetflow.20.7.1.N.016	Configure netflow to monitor the tunnels egress using routing protocol bgp	Configure netflow to monitor the tunnels egress using routing protocol bgp	Passed	

Granular Role-Based Access Control for Feature Templates

Logical ID	Title	Description	Status	Defect ID
ENJ.RBAC.20.7.1.N.001	Check if usergroup creation UI with linear view for granular RBAC features, policy RBAC and template RBAC are categorized together	In the process of creating a usergroup check if UI with linear view for granular RBAC features, policy RBAC and template RBAC are categorized together	Passed	
ENJ.RBAC.20.7N.002	Configure RBAC CLI Add-On Template access for user group.	Configure granular permission granting a user group access to CLI Add-On Template	Failed	CSCwb63989, CSCwb64202
ENJ.RBAC.20.7N.003	Moving a user out of group with RBAC access to CLI Add-On feature Template to verify CLI Add-On feature Template is not accessible	Move a user from group with access to CLI Add-On feature Template and check the user doesn't have access to CLI Add-On Template	Passed	
ENJ.RBAC.20.7N.004	Moving a user out of Security group with RBAC access to SIG feature template to verify SIG feature template is not accessible	Move a user from Security group with access to SIG feature template and check the user doesn't have access to the SIG Template.	Passed	
ENJ.RBAC.20.7N.005	Removing a group's Role Based access to CLI Add-On Template to check CLI Add-On Template is not accessible	Remove a group's Role Based access to CLI Add-On Templateand check CLI Add-On Template is not visible for a user in the group	Passed	

ENJ.RBAC.20.7 N.006	Removing a group's Role Based access to Device CLI Template to check Device CLI Template is not accessible	Remove a group's Role Based access to Device CLI Templateand check Device CLI Template is not visible for a user in the group.	Passed	
ENJ.RBAC.20.7 N.007	Removing a group's Role Based write access to Device CLI Template to confirm no write access to Device CLI Template	Remove a group's Role Based write access to Device CLI Templateand check Device CLI Template's Edit/ change device models/copy /delete functions are not visible for a user in the group.	Failed	CSCwb65298
ENJ.RBAC.20.7 N.008	Removing a group's Role Based access to SIG Template to check SIG Template is not accessible	Remove a group's Role Based access to SIG Templateand check SIG Template is not visible for a user in the group.	Failed	CSCwb65489
ENJ.RBAC.20.7 N.009	Usergroup RBAC in old releases upgrades to 20.7 granular RBAC	Upgrade to vManage 20.7 and see if old usergroup's RBAC access is upgraded to 20.7 granular RBAC	Passed	
ENJ.RBAC.20.7 N.010	Upgrade to vManage 20.7 and see if old usergroup's RBAC access is upgraded to 20.7 granular RBAC	Check if GET dataservice /template /feature/object/{templateId} API call executes successfully for Security group user with SIG Template access	Passed	
ENJ.RBAC.20.7 N.011	Check ifGET usergroup API call returns new RBAC features in header	Check if GET dataservice/admin /usergroup API call returns new RBAC features in header/viewControl[task]/controlData/data array	Passed	
ENJ.RBAC.20.7 N.012	Check if DELETE API call successful for user with SIG Template access	Check if DELETE dataservice/template /feature/{template_id} API call executes successfuly for Security group user with SIG Template access	Passed	

ENJ.RBAC.20.7 N.013	Check if DELETE API call unsuccessful for user with only read access for SIG Template	Check if DELETE dataservice/template/ feature/{template_id} API call fails for Security group user with only read access for SIG Template	Passed	
ENJ.RBAC.20.7 N.014	Check if POST API call unsuccessful for user with only read access for SIG Template	Check if POST dataservice/template/ device/cli API call fails for Security group user with only read access for SIG Template	Passed	
ENJ.RBAC.20.7 N.015	Check if PUT API call unsuccessful for Security group user with only read access for SIG Template	Check if PUT dataservice/template /device/TemplateId API call fails for Security group user with only read access for SIG Template	Passed	
ENJ.RBAC.20.7 N.016	Check if GET API call returns new RBAC roles introduced in 20.7	Check if GET dataservice/client/ user/roles call executes successfuly and returns new RBAC roles introduced in 20.7.	Passed	
ENJ.RBAC.20.7 N.017	Check new fields "read_permission" and "write_permission" according to RBAC feature config returned for API call	Configure Device CLI Template and SIG Template with (“read permission” & “write permission”) and only “read permission” respectively. Check if API call GET dataservice/template/ feature/types/ executes successfully and returns appropriate permissions for Device CLI Template and SIG Template	Passed	

RIPv2 support on Cisco IOS XE SD-WAN Devices

Logical ID	Title	Description	Status	Defect ID
ENJ.RIPv2.20.7.1.N.001	Configure the RIPV2 neighbourship between WAN edge and service router	Configure the RIPV2 neighbourship between WAN edge and service router	Passed	
ENJ.RIPv2.20.7.1.N.002	Configure the RIPV2 by updating the timers in Both routers	Configure to change the RIPV2 by updating the timers by using CLI	Passed	
ENJ.RIPv2.20.7.1.N.003	Configure the Invalid time in RIPV2 for both routers	Configure to change the RIPV2 by invalid the timers by using CLI	Passed	
ENJ.RIPv2.20.7.1.N.004	Verify the RIPV2 by using hold down timer for both routers	Configure to change the RIPV2 by hold down the timers by using CLI	Passed	
ENJ.RIPv2.20.7.1.N.005	Configure the flush timer in the RIPV2 for both Routers	Configure to change the RIPV2 by hold down the timers by using CLI	Passed	
ENJ.RIPv2.20.7.1.N.006	Configure the RIPV2 by using authentication in routing protocol	Configure the authentication in routing protocal by using CLI	Passed	
ENJ.RIPv2.20.7.1.N.007	Configure the redistribute RIP router over OMP for one router to another	Configure the redistribute RIP router over OMP by using CLI	Passed	
ENJ.RIPv2.20.7.1.N.008	Verify the service side RIPV2 with Passive interface	Configure the service side RIPV2 with passive interface by using CLI	Passed	
ENJ.RIPv2.20.7.1.N.009	Configure the OMP to service side RIP with Route map	Configure the OMP to service side RIPV2 with route map by using CLI	Passed	

ENJ.RIPv2.20.7.1.N.010	Verify RIPv2 between SDWAN routers with redistribute-static configured	Configure the sdwan routers with redistribute static configured by using CLI	Passed	
ENJ.RIPv2.20.7.1.N.011	Configure RIPv2 routes summarization between two sd-wan routers	Configure the RIPV2 routes summarization between 2 routers	Failed	CSCwb23903
ENJ.RIPv2.20.7.1.N.012	Configure to enable RIPv2 on OMP route tag	Enable the RIPV2 on OMP route tag by using CLI	Passed	
ENJ.RIPv2.20.7.1.N.013	Sevice Side RIPv2 with modified distribute prefix list-->IN	RIPV2 with modified distribute prefixlist by using CLI	Passed	
ENJ.RIPv2.20.7.1.N.014	Configure the BFD for RIPV2 neighbour	Configure the BFD for RIPV2 neighbour by using CLI	Passed	
ENJ.RIPv2.20.7.1.N.015	Configure the redistribute RIP routes to OSPFV3	Configure the NATPool interface for VPN by using CLI	Passed	

SNMPv3 AES 256 - cEdge Platforms

Logical ID	Title	Description	Status	Defect ID
ENJ.SNMPv3.20.7.1.N.001	Configure SNMPv3 on Cisco cEdge Devices Using Cisco vManage	This test case is to Configure SNMPv3 on Cisco cEdge Devices Using Cisco vManage	Passed	
ENJ.SNMPv3.20.7.1.N.002	Configure the sha256 authentication Support for SMNPv3 on Cisco IOS XE Cat8k platforms using Cisco vManage	Configure the sha256 authentication Support for SMNPv3 on Cisco IOS XE Cat8k platforms using Cisco vManage	Passed	
ENJ.SNMPv3.20.7.1.N.003	Create user with aes-256-cfb-128 privacy level encryption and auth level SHA256 on Cisco SDWAN device	This test case is to Create user with aes-256-cfb-128 privacy level encryption and auth level SHA256 on Cisco SDWAN device	Passed	
ENJ.SNMPv3.20.7.1.N.004	Configure SNMPv3 on Cisco IOS XE SD-WAN Devices Using Cisco vManage	Configure SNMPv3 on Cisco IOS XE SD-WAN Devices Using Cisco vManage	Passed	
ENJ.SNMPv3.20.7.1.N.005	Configure SNMP with Encrypted Strings Using CLI Templates	Configure SNMP with Encrypted Strings Using CLI Templates	Failed	CSCwb67444
ENJ.SNMPv3.20.7.1.N.006	Upgrade existing user encryption details from "aes-cfb-128" to "aes-256-cfb-128" encryption level with authlevel SHA256	Upgrade existing user encryption details from "aes-cfb-128" to "aes-256-cfb-128" encryption level with authlevel SHA256	Failed	CSCwb22631
ENJ.SNMPv3.20.7.1.N.007	Configure SNMP on Cisco IOS XE SD-WAN Devices Using CLI	Configure SNMP on Cisco IOS XE SD-WAN Devices Using CLI	Failed	CSCwb62150

ENJ.SNMPv3.20.7.1.N.008	Configure and enable SNMPv3 notifications on Cisco IOS XE SD-WAN Devices Using CLI	Configure and enable SNMPv3 notifications on Cisco IOS XE SD-WAN Devices Using CLI	Passed	
ENJ.SNMPv3.20.7.1.N.009	Verify SNMP Traps on Cisco IOS XE SD-WAN Devices from CLI	Verify SNMP Traps on Cisco IOS XE SD-WAN Devices from CLI	Passed	
ENJ.SNMPv3.20.7.1.N.010	Configure SNMPv2 backward compatibility on Cisco cEdge Devices Using the CLI	Configure SNMPv2 backward compatibility on Cisco vEdge Devices Using the CLI	Passed	
ENJ.SNMPv3.20.7.1.N.011	Configure & Verify SNMP Traps on Cisco vEdge Devices	Configure SNMPv3 on Cisco IOS XE SD-WAN Devices Using Cisco vManage	Passed	
ENJ.SNMPv3.20.7.1.N.012	Configure SNMP Traps on Cisco cEdge Devices	Configure SNMP Traps on Cisco cEdge Devices	Passed	
ENJ.SNMPv3.20.7.1.N.012	Validate different snmp client utilities like snmpwalk, snmpget, snmpgetnext, snmptrap with "aes-256-cfb-128" privacy level encryption and SHA256 auth level for Cisco SDWAN devices	Validate different snmp client utilities like snmpwalk, snmpget, snmpgetnext, snmptrap with "aes-256-cfb-128" privacy level encryption and SHA256 auth level for Cisco SDWAN devices	Passed	
ENJ.SNMPv3.20.7.1.N.013	Configure SNMP Traps on Cisco cEdge Devices	Configure SNMP Traps on Cisco cEdge Devices	Passed	
ENJ.SNMPv3.20.7.1.N.014	Validate the same SNMPv3 username for multiple times with and without encryption	Validate the same SNMPv3 user name for multiple times with and without encryption	Passed	

ENJ.SNMPv3.20.7.1.N.015	Validate the AES256 bit support along with AES 128bit support in SNMPv3 in vManage	Validate the AES256 bit support along with AES 128bit support in SNMPv3 in vManage	Passed	

Extended Visibility with Cisco SD-WAN and Cisco Thousand-Eyes

Logical ID	Title	Description	Status	Defect ID
ENJ.1000Eyes.20.7.1.N.001	Upload and configure Cisco ThousandEyes Enterprise Agent Software to Cisco vManage.	Configure and upload the ThousandEyes Enterprise Agent Software to Cisco vManage. \u0007	Passed	
ENJ.1000Eyes.20.7.1.N.002	Upload and configure Cisco ThousandEyes Enterprise Agent Software by devcie CLI method.	Configure and upload the ThousandEyes Enterprise Agent Software . \u0007	Passed	
ENJ.1000Eyes.20.7.1.N.003	Configure cisco ThousandEyes Enterprise Agent in VPN 0 for more visibility into the performance of underlay networks.	Configure and upload the ThousandEyes Enterprise Agent VPN \u0007 by using CLI	Passed	
ENJ.1000Eyes.20.7.1.N.004	Configure cisco ThousandEyes Enterprise Agent in a Service VPN by using vManage for more visibility into the performance of the Cisco SD-WAN overlay and underlay networks.	Configure and upload the ThousandEyes Enterprise Agent VPN \u0007	Passed	
ENJ.1000Eyes.20.7.1.N.005	Configure cisco ThousandEyes Enterprise Agent in a Service VPN using CLI for more visibility into the performance of the Cisco SD-WAN overlay and underlay networks.	Configure and upload the ThousandEyes Enterprise Agent VPN \u0007	Passed	

ENJ.1000Eyes.20.7.1.N.006	Upgrade Cisco ThousandEyes Enterprise Agent Software Automatically via vManage software repository.	Configure and upgrade the ThousandEyes Enterprise Agent Software \u0007	Passed	
ENJ.1000Eyes.20.7.1.N.007	Upgrade ThousandEyes whole package software by vManage & CLI.	Configure and Upgrade the ThousandEyes whole package Software \u0007	Passed	
ENJ.1000Eyes.20.7.1.N.008	Extend visibility with sdwan and thousandeyes to enable automated routing based on the network performance & availability. \u0007	Configure the ThousandEyes to enable the automated routing \u0007	Failed	CSCwb65635
ENJ.1000Eyes.20.7.1.N.009	Extend network visibility between the branch and DC (point to point network metrics).	Configure ThousandEyes and extend network between branch to DC \u0007	Passed	
ENJ.1000Eyes.20.7.1.N.010	Configure cisco ThousandEyes Enterprise Agent by vManage CLI template	Configure and upload the ThousandEyes Enterprise Agent Software . \u0007	Failed	CSCwb65614
ENJ.1000Eyes.20.7.1.N.011	Configure ThousandEyes agent via CLI and enable NAT on DIA interface and check the TE traffic via DIA.	Configure and upload the ThousandEyes and enable NAT on DIA interface. \u0007	Passed	
ENJ.1000Eyes.20.7.1.N.012	Configure UTD and ThounsandEyes in the same device and check the behaviour.	Configure the ThousandEyes and UTD in the same device \u0007	Passed	

ENJ.1000Eyes.20.7.1.N.013	Configure the ThousandEye Agent with default hostname & modify to some other hostname and check the behaviour..	Configure the ThousandEyes default hostname & modify \u0007 by using vManage	Failed	CSCwb53554 , CSCwb55473
ENJ.1000Eyes.20.7.1.N.014	Configure cisco ThousandEyes Enterprise Agent in VPN 0 & VPN 100 for more visibility into the performance of underlay & underlay networks	Configure ThousandEyes Enterprise Agent in VPN 0 & VPN 100 for more visibility \u0007 by using CLI	Passed	

TCP-UDP port tracker for static route

Logical ID	Title	Description	Status	Defect ID
ENJ.PortTracker.20.7.1.N.001	Configure the Single Static Route to Track the Endpoint	Configured the single track for static route by using CLI	Passed	
ENJ.PortTracker.20.7.1.N.002	Configured the single track for static route	Configured the TCP port tracker for static route by using CLI	Passed	
ENJ.PortTracker.20.7.1.N.003	Configure the TCP/UDP port tracker with tracker group for static route	Configure the TCP/UDP port tracker by using CLI	Passed	
ENJ.PortTracker.20.7.1.N.004	Configure the UDP port Tracker for Static Route endpoint	Configured the UDP port tracker for static route by using CLI	Passed	
ENJ.PortTracker.20.7.1.N.005	Configure the tracking group with TCP/UDP port tracking by using Boolean operation (AND)	Configure the TCP/UDP port tracker by using CLI	Passed	
ENJ.PortTracker.20.7.1.N.006	Configure the combination of TCP port tracker and static route by using tracking group with default Boolean operation	Configure the TCP/UDP port tracker by using CLI	Passed	
ENJ.PortTracker.20.7.1.N.007	Configure the modification of multiple/threshold /interval parameters Instead of default values	Modified the values by using CLI	Failed	CSCwb61835
ENJ.PortTracker.20.7.1.N.008	Configure the single UDP port tracker and static route with tracking group by using Boolean operation (AND)	Configure the single UDP port tracker with static route by using CLI	Passed	

ENJ.PortTracker.20.7.1.N.009	Configure the combination of TCP/UDP port tracker with DNS by using tracking group	Configure the TCP/UDP port tracker with DNS by using vManage	Passed	
ENJ.PortTracker.20.7.1.N.010	Configure the UDP port tracker with DNS tracker by using tracking group with Boolean operationàAND	Configure the UDP port tracker with DNS by using vManage	Failed	CSCwb61935
ENJ.PortTracker.20.7.1.N.011	TCP/UDP port tracker for static route with tracking group by using VManage	Configure the TCP/UDP port tracker by using vManage	Passed	
ENJ.PortTracker.20.7.1.N.012	Configure the TCP/UDP tracker with tracking group by using VManage	Configure the TCP/UDP port tracker with Boolean operation (AND) by using vManage	Passed	
ENJ.PortTracker.20.7.1.N.013	Configure the single UDP port tracker with IP Address by using VManage	Configure the TCP/UDP port tracker with Boolean operation (AND)	Passed	
ENJ.PortTracker.20.7.1.N.014	Configure the TCP port tracker with IP Address by using VManage	Configure the TCP port tracker with IP Address	Passed	

UX 2.0 Monitoring

Logical ID	Title	Description	Status	Defect ID
ENJ.UX2Monitor.20.7.1.N.001	Monitor the Main dashboard & monitor the site health & status of controllers & edge device	Configure the site health and status of controllers and edge device by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.002	Monitor Device & verify the Device status	Configure the device status by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.003	Monitor Device & verify the device status - Colocation cluster	Configure the device status of colocation cluster by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.004	Monitor Device & verify the device status - certificate	Configure the device status of certificate by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.005	Monitor Device & verify the device status - Licensing	Configure the device status of Licensing by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.006	Monitor Tunnels & verify the tunnels status	Configure the tunnels status by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.007	Monitor Security & verify the security status - Firewall Enforcement	Configure the security status - Firewall Enforcement by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.008	Monitor VPN & verify the VPN option	Configure the VPN status by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.009	Monitor Multicloud & verify the Multicloud option	Configure the Multicloud option by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.010	Monitor Log & verify the Log option - Alarm	Configure the log option with Alarm by using vManage	Passed	

ENJ.UX2Monitor.20.7.1.N.011	Monitor Log & verify the Log option - Events	Configure the log option with Events by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.012	Monitor Log & verify the Log option - Audit Log	Configure the log option with Audit log by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.013	Monitor Log & verify the Log option - ACL Log	Configure the log option with ACL Log by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.014	Monitor Security & verify the security option - Top Signature Hits	Configure the security status in Top Signature Hits by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.015	Monitor Security & verify the security option - Advanced Malware Protection	Configure the security status in Advanced Malware Protection by using vManage	Passed	
ENJ.UX2Monitor.20.7.1.N.016	Monitor Security & verify the security option - URL Filtering	Configure the security status in URL Filtering by using vManage	Passed	

GRE Over IPsec Tunnels Between Cisco IOS XE Devices

Logical ID	Title	Description	Status	Defect ID
ENJ.GreOverIpsec.20.7.1.N.001	Configure GRE Tunnel from SDWAN Branch to non SDWAN DC Site	To Configure GRE Tunnel from SDWAN branch site to DC with non SDWAN Set up.	Passed	
ENJ.GreOverIpsec.20.7.1.N.002	Configure GRE Tunnel from non SDWAN branch to non SDWAN DC	To Configure GRE Tunnel from non SDWAN branch to non SDWAN DC	Passed	
ENJ.GreOverIpsec.20.7.1.N.003	Configure GRE Over IPsec Tunnels Between SDWAN Branch to non SDWAN DC Site	You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast (in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations.	Passed	

ENJ.GreOverIpsec.20.7.1.N.004	Monitor GRE Over IPsec Tunnels Between SDWAN Branch to non SDWAN DC Site	You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast (in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations.	Passed	

ENJ.GreOverIpsec.20.7.1.N.005	Configure GRE Over IPsec Tunnels Between Non SDWAN IOS XE branch to Non SDWAN DC Site.	You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast (in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations.	Passed	

ENJ.GreOverIpsec.20.7.1.N.006	Monitor GRE Over IPsec Tunnels Between Non SDWAN IOS XE branch to Non SDWAN DC Site.	You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast (in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations.	Passed	

ENJ.GreOverIpsec.20.7.1.N.007	To verify OSPF v3 traffic from SDWAN Branch site to non SDWAN Data center.	You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast (in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations.	Passed	

ENJ.GreOverIpsec.20.7.1.N.008	To Verify Multicast Traffic from SDWAN Branch site to non SDWAN Data Center site.	You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast (in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations.	Passed	

ENJ.GreOverIpsec.20.7.1.N.009	To Verify BGP Traffic from SDWAN Branch site to non SDWAN Data Center site.	You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast (in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations.	Passed	

ENJ.GreOverIpsec.20.7.1.N.010	BGP with metric configured and to verify the traffic flow from SDWAN branch to SDWAN DC.	You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast (in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations.	Passed	

ENJ.GreOverIpsec.20.7.1.N.011	To Analysis the behavior of flapping tunnel on GRE over IPsec from branch to DC.	You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast (in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations. \u0007	Passed	

ENJ.GreOverIpsec.20.7.1.N.012	Failover of duel MPLS WAN link on GRE over IPSEC Tunnel	You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast (in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations.	Passed	

ENJ.GreOverIpsec.20.7.1.N.013	To verify OSPF v3 traffic from non SDWAN Branch site to non SDWAN Data center	You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast (in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations.	Passed	

ENJ.GreOverIpsec.20.7.1.N.014	To Configure and Verify Crypto PKI Certificate on cEdge router.	You can configure Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel on Cisco IOS XE devices. GRE supports multicast and dynamic routing protocol, IPsec with IKEv2 protocol offers the enhanced security. GRE over IPsec tunnels are configured using the OSPFv3(dynamic routing protocol) and multicast (in sparse-mode), using the IPsec to encrypt the packets across the tunnels, and using the IKEv2 along with RSA-SIG authentication to perform authentication, establish and maintain security associations.	Passed	
ENJ.GreOverIpsec.20.7.1.N.014	To Verify VPN 100 and 200 traffic from SDWAN Site to Non SDWAN DC with GRE over IPsec.	To Configure VPN 100 and 200 traffic from SDWAN Site to Non SDWAN DC with GRE over IPsec.	Passed	

Regression Features

SLA Classes

Logical ID	Title	Status	Defect Id
ENJ.SLA Classes.20.7.1.N.001	Configuring App Aware Routing with DSCP 10 values in SLA Class	Passed	
ENJ.SLA Classes.20.7.1.N.002	Configuring App Aware Routing with DSCP 12 values in SLA Class	Passed	
ENJ.SLA Classes.20.7.1.N.003	Configuring App Aware Routing with DSCP 14 values in SLA Class	Passed	
ENJ.SLA Classes.20.7.1.N.004	Configuring Source and destination port in app aware routing using DSCP 10 values in SLA Class	Passed	
ENJ.SLA Classes.20.7.1.N.005	Configuring Source and destination port in app aware routing using DSCP 12 values in SLA Class	Passed	
ENJ.SLA Classes.20.7.1.N.006	Configuring Source and destination port in app aware routing using DSCP 14 values in SLA Class	Passed	
ENJ.SLA Classes.20.7.1.N.007	Configuring Google DNS application list in app aware routing using DSCP values in SLA Class	Passed	
ENJ.SLA Classes.20.7.1.N.008	SLA Data Traffic monitoring based on Jitters, Loss and latency.	Passed	
ENJ.SLA Classes.20.7.1.N.009	Verify whether the SLA Data Traffic monitoring based on 10 ms Jitters, 10% Loss and 50ms latency.	Passed	

ENJ.SLA Classes.20.7.1.N.010	Verify whether the SLA Data Traffic monitoring based on 20 ms Jitters, 20% Loss and 100ms latency.	Passed	
ENJ.SLA Classes.20.7.1.N.011	Verify whether SLA Data Traffic monitoring based on 50ms Jitters, 50% Loss and 150ms latency.	Passed	
ENJ.SLA Classes.20.7.1.N.012	Verify whether SLA Data Traffic monitoring based on 75ms Jitters, 75% Loss and 200ms latency.	Passed	
ENJ.SLA Classes.20.7.1.N.013	Verify whether SLA Data Traffic monitoring based on 85ms Jitters, 85% Loss and 250ms latency.	Passed	
ENJ.SLA Classes.20.7.1.N.014	Verify whether SLA Data Traffic monitoring based on 100ms Jitters, 100% Loss and 300ms latency.	Passed	
ENJ.SLA Classes.20.7.1.N.015	Creating SLA Classes in Centralized data policy.	Passed	

Per VPN QoS

Logical ID	Title	Status	Defect Id
ENJ.Per VPN QoS.20.7.1.N.001	To Configure per VPN Support QoS via CLI Template	Passed	
ENJ.Per VPN QoS.20.7.1.N.002	To Set 4 Class forwarding QoS policy under per VPN QoS	Passed	
ENJ.Per VPN QoS.20.7.1.N.003	Set Bandwidth for Multiple VPN using per VPN QoS policy and verify Traffic goes as per VPN QoS policy	Passed	
ENJ.Per VPN QoS.20.7.1.N.004	Set 8 Class forwarding QoS policy under per VPN QoS and verify Traffic goes as per VPN QoS policy	Passed	
ENJ.Per VPN QoS.20.7.1.N.005	To Set combination of 4 and 8 Class forwarding QoS policy under per VPN QoS and verify Traffic goes as per VPN QoS policy	Passed	
ENJ.Per VPN QoS.20.7.1.N.006	Set for Multiple VPN under single VPN Group and verify Traffic goes as per VPN QoS policy	Passed	
ENJ.Per VPN QoS.20.7.1.N.007	Set for Multiple VPN under different VPN Group and verify Traffic goes as per VPN QoS policy	Passed	
ENJ.Per VPN QoS.20.7.1.N.008	To Configure Per VPN QoS using feature template via vManage and verify QoS works as per VPN policy	Passed	
ENJ.Per VPN QoS.20.7.1.N.009	To Multiple VPN under QoS VPN Group using CLI template via vManage	Passed	

ENJ.Per VPN QoS.20.7.1.N.010	To Adding a new QoS SLA class list, activating the policy, and attaching with device Template	Passed	

SIG Umbrella Tunnel

Logical ID	Title	Status	Defect Id
ENJ.SIG-Umbrella.20.7.1.N.01	Allow or Deny the Branch application traffic based on the application engine	Passed	
ENJ.SIG-Umbrella.20.7.1.N.02	Allow or Deny the Branch website traffic based on the category's engine	Passed	
ENJ.SIG-Umbrella.20.7.1.N.03	Allowing the sites based on the Destination lists – whitelist	Passed	
ENJ.SIG-Umbrella.20.7.1.N.04	Allowing and blocking the sites based on the Destination lists – Block list	Passed	
ENJ.SIG-Umbrella.20.7.1.N.05	Redirect the block page to default umbrella blocked page	Passed	
ENJ.SIG-Umbrella.20.7.1.N.06	Redirect the block page to the external block page and display with blocked by which category	Passed	
ENJ.SIG-Umbrella.20.7.1.N.07	Redirect the block page to the external block page and display with blocked based on destination list	Passed	
ENJ.SIG-Umbrella.20.7.1.N.08	Redirect the block page to the external block page and display with blocked based on phishing setting and security settings	Passed	
ENJ.SIG-Umbrella.20.7.1.N.09	Create an account and user role in the umbrella dashboard and assign the permissions	Passed	
ENJ.SIG-Umbrella.20.7.1.N.10	Bypass the blocked pages and applications for the specific users	Passed	
ENJ.SIG-Umbrella.20.7.1.N.11	Bypass the blocked pages and applications for the specific codes	Passed	

ENJ.SIG-Umbrella.20.7.1.N.12	To check the logs and download the log reports	Passed	
ENJ.SIG-Umbrella.20.7.1.N.13	Manual Network Tunnel configuration with cEdge and Umbrella	Passed	
ENJ.SIG-Umbrella.20.7.1.N.14	Automatic Network Tunnel configuration with cEdge and Umbrella	Passed	
ENJ.SIG-Umbrella.20.7.1.N.15	Cisco Umbrella SIG integration with cEdge via vManage	Passed	
ENJ.SIG-Umbrella.20.7.1.N.16	Cisco Umbrella SIG with Manual IPsec Tunnel	Passed	
ENJ.SIG-Umbrella.20.7.1.N.17	Configuring cloud-delivered firewall and filter traffic at layer 3 and layer 4 and layer 7	Passed	
ENJ.SIG-Umbrella.20.7.1.N.18	Enable File Inspection for DNS Policies	Passed	
ENJ.SIG-Umbrella.20.7.1.N.19	Enable File Inspection for WEB Policies	Passed	
ENJ.SIG-Umbrella.20.7.1.N.20	Umbrella Integration Using CLI	Passed	
ENJ.SIG-Umbrella.20.7.1.N.21	Configure Static Routes	Passed	
ENJ.SIG-Umbrella.20.7.1.N.22	Single branch single edge having Dual DIA link & Configuring CoR SAAS and the internet exit point as a SIG Auto tunnel interface (Active-Active)	Passed	

Cloud on Ramp SaaS Secure Internet Gateway Interface

Logical ID	Title	Status	Defect Id
ENJ.Saas-Sec-Gateway-Int.20.7.1. N.1	Single DIA link SAAS traffic exit via Sig Auto tunnel	Passed	
ENJ.Saas-Sec-Gateway-Int.20.7.1. N.2	Single DIA link SAAS traffic exit via Sig Manual tunnel	Passed	
ENJ.Saas-Sec-Gateway-Int.20.7.1. N.3	Single DIA link SAAS traffic exit via Sig Auto tunnel with manually enabled tracker	Passed	
ENJ.Saas-Sec-Gateway-Int.20.7.1. N.4	Single DIA link SAAS traffic exit via Sig Manual tunnel with manually enabled tracker	Passed	
ENJ.Saas-Sec-Gateway-Int.20.7.1. N.5	Single edge with DIA & GW, DIA goes down traffic via GW with SIG Auto Tunnel	Passed	
ENJ.Saas-Sec-Gateway-Int.20.7.1. N.6	Single edge with DIA & GW, DIA goes down traffic via GW with SIG Manual Tunnel	Passed	
ENJ.Saas-Sec-Gateway-Int.20.7.1. N.7	Single edge with DIA & GW, DIA goes down traffic via GW with SIG Manual Tunnel	Passed	
ENJ.Saas-Sec-Gateway-Int.20.7.1. N.8	Single GW link SAAS application Traffic via SIG Manual Tunnel	Passed	
ENJ.Saas-Sec-Gateway-Int.20.7.1. N.9	Single GW link SAAS application Traffic via SIG Manual Tunnel	Passed	

ENJ.Saas-Sec-Gateway-Int.20.7.1. N.10	Single GW link SAAS traffic exit via Sig Manual tunnel with manually enabled tracker	Passed	
ENJ.Saas-Sec-Gateway-Int.20.7.1. N.11	Single GW link SAAS traffic exit via Sig Auto tunnel with manually enabled tracker	Passed	

Related Documents

Related Documentation

Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release 17.7 Release Notes

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/xe-17-7/sd-wan-rel-notes-xe-17-7.html#concept_yhf_b5y_jsb

Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.7

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/ios-xe-17/systems-interfaces-book-xe-sdwan/m-hot-standby-router-protocol.html

Cisco SD-WAN NAT Configuration Guide, Cisco IOS XE Release 17.7

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/nat/nat-book-xe-sdwan/configure-nat.html#intra-vpn-service-side-nat

Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.7

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/traffic-flow-monitor.html

Cisco SD-WAN Routing Configuration Guide, Cisco IOS XE Release 17.7

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/m-unicast-routing.html#Cisco_Concept.dita_Routing-Information-Protocol-Overview

Cisco SD-WAN SNMP Configuration Guide

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/snmp/snmp-book/snmp-book_2.html#Cisco_Concept.dita_Configure-SNMPv3-on-IOS-XE-Devices-Using-Cisco-vManage

Cisco SD-WAN Security Configuration Guide, Cisco IOS XE Release 17.7

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/m-gre-over-ipsec-tunnels.html