Test Results Summary for IOS XE SD-WAN for Japan (Release Version 20.12.1/17.12.1)

First Published: 2023-08-08

Last Modified: 2023-08-25

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

CHAPTER 1 **Overview** 1

Cisco IOS XE SD-WAN 2

CHAPTER 2 **Test topology and Environment Matrix** 5

Test Topology 6

Component Matrix 7

What's New ? 8

Open Caveats 9

Resolved Caveats 12

CHAPTER 3 **New Features** 13

Support for Dual Device Site Configuration 14

Global Network View with Network-Wide Path Insight Integration 20

vManage - Security Enhanced dashboard 22

Cisco Catalyst SD-WAN Remote Access Configuration in SSL-VPN Mode 25

Symmetric Routing-Management Region-intent based hub-spoke-On-demand tunnels with TGW 29

Enabling MACsec using Cisco SD-WAN 34

IPv6 GRE-IPSEC Tunnels to Third party-Generic Integration 37

Cat8K and ISR1K-Trustsec SDA-SDWAN Scale Measurement 41

Improved Brownout detection and Traffic steering 44

Routing vManage base automation for Autonomous mode 46

Sr cfd 49

CHAPTER 4 **Regression Features** 55

NAT 56

DIA 60

AAR and VPN Segmentation 62
TLOC 65
Path MTU 67
Vmanage UI 69
SD-AVC 71
SDRA 72
QoS 74
Adhoc 77

CHAPTER 5 **Related Documents** 79
Related Documentation 80

Overview

- **Cisco IOS XE SD-WAN** , on page 2

Cisco IOS XE SD-WAN

Cisco SD-WAN IOS XE 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 20.12.1 - IOS XE 17.12.1
- 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
- ESXi Host 6.5
- Cisco Catalyst 8300
- Cisco Catalyst 8200
- Cisco Catalyst 8500L
- Cisco ISR 4461
- Cisco Catalyst 9K PoE Switch
- Cisco Catalyst 1111-8P

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

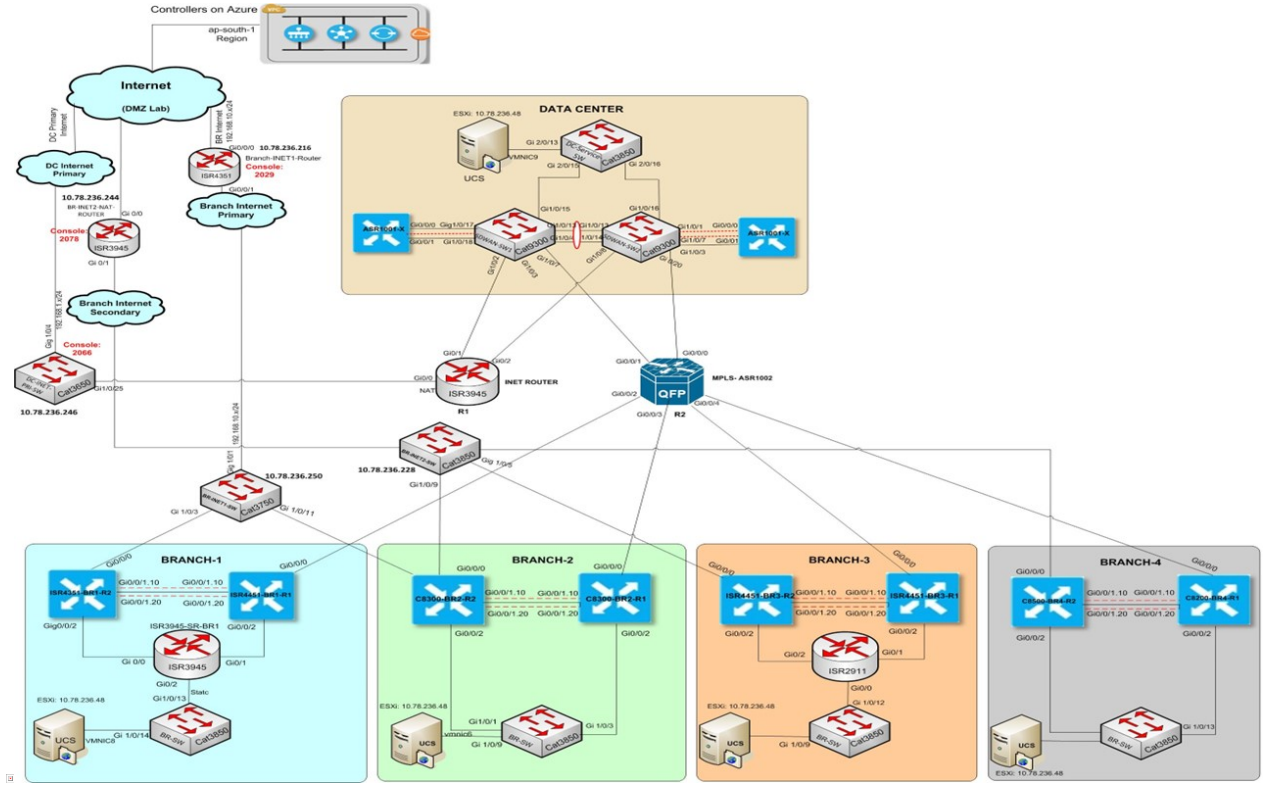
CA	Certificate Authority
CDF	Cloud Delivered Firewall
cEdge Router	Cisco Edge Router
Cisco DNA	Cisco Digital Network Architecture
Config	Configuration
Config-t	Configuration-transaction
COM Port	Communication Port
CoR	Cloud on Ramp
CLI	Command Line
CSP	Cisco Cloud Services Platform
DC	Data Center
DHCP	Dynamic Host Configuration Protocol
DIA	Direct Internet Access
DR	Disaster Recovery
DSCP	Differentiated Services Code Point
Dst	Destination
EF	Expedited Forwarding
EIGRP	Enhanced Interior Gateway Routing Protocol
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
FW	Firewall
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
INET	Internet
IOS	Internetworking Operating System
IPS	Intrusion prevention system
ISR	Integrated Services Routers

LAN	Local Area Network
MAN	Metropolitan Area Network
MPLS	Multi-Protocol Label Switching
ISE	Identity Services Engine
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, on page 6
- Component Matrix, on page 7
- What's New ?, on page 8
- Open Caveats, on page 9
- Resolved Caveats, on page 12

Test Topology



Component Matrix

Applications	Category	Component	Version
Controller Network	Virtual Network	vBond	20.12.1
		vManage	20.12.1
		vSmart	20.12.1
	Switch	Cat 9K PoE	17.2
Communications Infrastructure	IOS XE SDWAN	C8300, C8200,C8500 & C8500L	17.12.1
		ISR4461	17.12.1
UCS	UCSC-C240-M5SX	ESXi Host	6.0, 6.5
Client	Operating System	End point	Windows 10
	Browsers	Mozilla	115.0.2
		Chrome	115.0.5790.102

What's New ?

SDWAN 20.12.1 - IOS XE 17.12.1 Solution testing

- Support for Dual Device Site Configuration
- Global Network View with Network-Wide Path Insight Integration
- vManage - Security Enhanced dashboard
- Cisco Catalyst SD-WAN Remote Access Configuration in SSL-VPN Mode
- Symmetric Routing, Management Region, intent based hub-spoke, On-demand tunnels with TGW
- Enabling MACsec using Cisco SD-WAN Manager
- IPv6 GRE/IPSEC Tunnels to Third party – Generic Integration
- Cat8K and ISR1K – Trustsec (SDA-SDWAN) Scale Measurement
- Improved Brownout detection and Traffic steering
- Routing vManage base automation for Autonomous mode
- SR CFD

Open Caveats

CDETS ID	Title
CSCwf62681	C8200/C8300 Devices are going down to Roman Mode while Reboot Log:"TAM_LIB_ERR_WRITE_FAILURE"
CSCwf73767	Add Service VPN Template UI Page is Freezed and Overlaid/Reflecting on all over the vManage.
CSCwf51256	Select Range Button is not clickable to Select the Site ID's Range.
CSCwf44757	Can't Able to Create a Topology with Empty Record under Configuration.
CSCwf39120	Can't able to Add URL Filtering Under Group of Interest.
CSCwf32045	Info (i) button is replicated & displayed Incorreclty in another page.
CSCwf54278	Incorrect/Irrelevant path is being displayed under Devices > System Status > Reboot.
CSCwf54260	Incorrect/Irrelevant path is being displayed under Devices > System Status > Crash.
CSCwf51333	Workflow > Quick Connect Header is displaying Incorrect/Other Header.
CSCwf44809	Priority Selected Site List Pop Up is displaying Incorrectly under Add Spoke Group.
CSCwf40878	Background UI Scroll Bar is visible in other Foreground UI Pane / Scroll Bar isn't Working.
CSCwf40817	Can't Able to Choose/Unchoose the Options due to overlay of Apply/Cancel.
CSCwh01097	Clicking on the Device Hostname is been redirected to Incorrect/Irrelevant Page.
CSCwf22563	Path Mismatch for Security Policies/Profiles under Configurations.
CSCwf40903	vManage GUI isn't detecting the USB Stick Connected to a particular device slot.
CSCwf85947	Zscalar registration Enabled by Wrong User ID ,User name not should be Integer.
CSCwf42521	Certificate Authority (CA) Settings View and Edit button is not working.
CSCwf67086	The Device template failed when attached the device

CSCwh03140	In Zscler registration for "Partner base URl" filed accepted Numeric values
CSCwh03750	After Umbrella registration in Vmanage when try to get key for token we are getting error
CSCwf77155	PMT credentials When Enabled/disabled in Vmanage ,its not displayed Enabled/disabled.
CSCwf77138	Smart Account credentials When Enabled/disabled in Vmanage ,its not display Enabled/disabled.
CSCwf63724	"SD-AVC Cloud connector When disabled in Vmanage ,its not display disabled in Administration Settings"
CSCwf71122	Security page is Malfunctioning - Not working as expected - Chrome and Firefox
CSCwf72625	Software Repository page is Malfunctioning - Not working as expected - Chrome and Firefox browser
CSCwf72695	Administration -> License Management page is Malfunctioning - Chrome and Firefox browser
CSCwf72638	Software Repository - Firmware page is Malfunctioning - Chrome and Firefox browser
CSCwf71058	Issue with scroll bar - Chrome browser - Device - Export option
CSCwf71176	Issue with scroll bar - Firefox - Configuration -> Certificate Authority
CSCwf71165	Issue with scroll bar - Chrome & Firefox browser - Device - Export option
CSCwf71095	Issue with scroll bar - Chrome browser - Security - Advanced Malware Protection
CSCwf84342	In Eigrp feature profile,Able to create the authentication key with empty space characters
CSCwh01078	Copy of configuration group with Dual device type is creating with single router type.
CSCwh02446	Accepting duplicate tag name after editing the created configuration group.
CSCwf84317	Allowing to create view with empty character values under SNMP feature in feature templates.
CSCwf84727	Unable to add IPS signature as per the Hint provided.
CSCwh01068	For view details option, the field values must be Greyed out.
CSCwf84274	Grouping fields option is missing in new trace(nwpi) using geographic view

CSCwf76221	Clicking the hyperlink of the device hostname is been redirected to incorrect/irrelevant page
CSCwf75918	Policy still exists even after successful deletion
CSCwf88277	Unable to attach Device in the feature template

Resolved Caveats

CDETS ID	Title
CSCwf63112	Can't Able to edit the user group's created under Administration > Manage Users.
CSCwf58039	Install Button & Select File button is not functioning Properly to add Certificates.
CSCwf43710	Cloud onRamp for SaaS > Application and Policy Page not loading on refresh
CSCwf36632	Save Policy Options were Overlaid & making inconvenient with the other required configurations.
CSCwf36616	Couldn't able to Click Import Option for Adding Prefix List.
CSCwf22638	Custom options drop-down is persisting in the next screen/page.
CSCwf37830	Path is Invisible & SAIE Applications Path is displaying Incorrectly.
CSCwf50047	Root CA Management Page is Overlaid/Reflected on all the other pages.
CSCwf58010	Options in the Gear/Settings Button is disabled Automatically.
CSCwf67622	vManage is loading continuously when a new user access is created with Network Hieracrchy.
CSCwf69085	Unable to Add new T1/E1 interface in VPN interface multilink feature in configuration group

New Features

- Support for Dual Device Site Configuration, on page 14
- Global Network View with Network-Wide Path Insight Integration, on page 20
- vManage - Security Enhanced dashboard, on page 22
- Cisco Catalyst SD-WAN Remote Access Configuration in SSL-VPN Mode , on page 25
- Symmetric Routing-Management Region-intent based hub-spoke-On-demand tunnels with TGW, on page 29
- Enabling MACsec using Cisco SD-WAN, on page 34
- IPv6 GRE-IPSEC Tunnels to Third party-Generic Integration, on page 37
- Cat8K and ISR1K-Trustsec SDA-SDWAN Scale Measurement, on page 41
- Improved Brownout detection and Traffic steering, on page 44
- Routing vManage base automation for Autonomous mode, on page 46
- Sr cfd, on page 49

Support for Dual Device Site Configuration

Logical ID	Title	Description	Status	Defect ID
ENJ.Config.2.0.12.1_17.12.1_N.01	To build a Configuration Group supporting dual device sites using Simple Configuration workflow.	Creating a configuration group through configuration workflow which supports the site type with dual devices.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.02	To add/remove existing Site IDs/Site Names from existing Configuration Group in workflow.	Checking whether able to add or remove the site IDs and site names from the existing Configuration Group in workflow	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.03	To modify existing “Active” or “Secondary” values assigned to devices.	Check whether able to modify the existing “Active” or “Secondary” values assigned to devices.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.04	To create a QoS Map Policy via workflow policy profile	Configuring a Qos Map policy using workflow of configuration group under policy profile.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.05	To create a Default AAR/SLA Policy using policy	Configuring an AAR/SLA policy using workflow of configuration group under policy profile.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.06	To create a DIA Policy via Simple workflow policy profile.	Configuring a DIA policy using workflow of configuration group under policy profile.	Passed	

ENJ.Config.2.0.12.1_17.12.1_N.07	To create a SIG Policy via Simple workflow policy profile.	Configuring a SIG policy using workflow of configuration group under policy profile.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.08	To create a Routing Policy via Simple workflow policy profile	Configuring a Routing policy using workflow of configuration group under policy profile.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.09	To create a DSL IPOE, feature parcel under Transport &management profile	In Transport &management profile, creating a DSL IPoE feature	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.10	To create a DSL PPoE, feature parcel under Transport &management profile	In Transport &management profile, creating a DSL PPoE feature	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.11	To create a DSL PPPoE, feature parcel using PAP protocol under Transport &management profile.	In Transport &management profile, creating a DSL PPPoE feature with protocol type as PAP protocol	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.12	To create a DSL PPPoE, feature multiple times under Transport &management profile.	Creating a DSL PPPoE feature multiple times under Transport &management profile in the existing configuration group	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.13	To associate a tracker for DSL PPPoE, feature parcel.	In Transport &management profile, creating a DSL PPPoE feature and associate a tracker for DSL PPPoE feature	Passed	

ENJ.Config.2.0.12.1_17.12.1_N.14	To create a DSL PPPoA, feature parcel using CHAP protocol under Transport &management profile.	In Transport &management profile, creating a DSL PPPoA feature with protocol type as CHAP protocol.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.15	To create a DSL PPPoA, feature parcel multiple times under Transport &management profile.	Creating a DSL PPPoA feature multiple times under Transport &management profile in the existing configuration group	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.16	To create a DSL PPPoA, feature parcel using ipsec tunnel encapsulation under Transport &management profile	In Transport &management profile, creating a DSL PPPoA feature.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.17	To associate a tracker for DSL PPPoA feature.	In Transport &management profile, creating a DSL PPPoA feature and associate a tracker for DSL PPPoA feature	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.18	To check Ethernet PPPoE can be crated multiple times under VPN0	Checking whether able to create a multiple times Ethernet PPPoE feature under VPN0 in transport and management profile.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.19	To create an Ethernet PPPoE feature using CHAP&PAP protocol under Transport &management profile.	In Transport &management profile, creating a Ethernet PPPoE feature with protocol type as CHAP &PAP protocol.	Passed	

ENJ.Config.2.0.12.1_17.12.1_N.20	To create an Ethernet PPPoE, feature tunnel using GRE encapsulation under Transport &management profile	In Transport &management profile, creating an Ethernet PPPoE feature tunnel using GRE encapsulation.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.21	To associate a tracker for Ethernet PPPoE feature.	In Transport &management profile, creating a Ethernet PPPoE feature and associate a tracker for Ethernet PPPoE feature	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.22	To configure an EIGRP feature in service profile	Creating an eigrp feature under service profile in the existing configuration group.	Failed	CSCwf84342
ENJ.Config.2.0.12.1_17.12.1_N.23	To create a multiple eigrp feature parcels under service profile.	Creating a multiple eigrp feature under service profile in the existing configuration group.	Failed	CSCwf84342
ENJ.Config.2.0.12.1_17.12.1_N.24	To create a flexible port speed parcel under system profile.	Creating a flexible port speed parcel under system profile in the existing configuration group.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.25	To create object tacker using interface.	Creating an object tracker with tracker type using interface	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.26	To associate the object tracker with vrrp shutdown.	Associating an object tracker under service profile with vrrp shutdown.	Passed	

ENJ.Config.2.0.12.1_17.12.1_N.27	To create a VPN Interface Multilink Feature parcel under Service profile	Creatin a VPN interface Multilink feature under Service profile using configuration group.	Passed	CSCwf69085
ENJ.Config.2.0.12.1_17.12.1_N.28	To create a multiple VPN Interface Multilink Feature parcel under Transport profile	To create a multiple VPN Interface Multilink Feature under Transport profile	Passed	CSCwf69085
ENJ.Config.2.0.12.1_17.12.1_N.29	To configure the VRF Route leak feature parcel Transport VPN to Service VPN	Configuring the VRF Route leak feature in service level VPN from Transport VPN to Service VPN.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.30	To configure the VRF Route leak feature Service VPN to Service VPN	Configuring the VRF Route leak feature in service level VPN from Service VPN to Service VPN.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.31	To create a centralized policy for SLA class using vmanage	Configuring a centralized policy with sla class.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.32	To create a Centralized policy with protocol rule using vmanage	Configuring a centralized policy with protocol rule using in Application aware routing via vmanage.	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.33	To create a centralized Policy to forward to a TLOC color for the application family.	Configuring a centralized Policy to forward to a TLOC color for the application family	Passed	
ENJ.Config.2.0.12.1_17.12.1_N.34	To create a snmp feature using feature template.	configuration a snmp feature through configuration with fetaure templates	Failed	CSCwf84317

ENJ.Config.2.0.12.1_17.12.1_N.35	To create a copy of existing configuration group with dual device type	With existing configuration with dual device type ,cretae a copy of configuration group	Failed	CSCwh01078
ENJ.Config.2.0.12.1_17.12.1_N.36	To create a security policy with advanced ips signature list.	Configure a security policy ,by including the advanced ips signature list.	Failed	CSCwf84727
ENJ.Config.2.0.12.1_17.12.1_N.37	To associate a device tag names for dual device type in configuration group	Create a configuration group with dual device type and associate the device with device tag names	Failed	CSCwh02446
ENJ.Config.2.0.12.1_17.12.1_N.38	To view the existing T1E1 Controller feature details.	Create a configuration group with T1E1 controller feature and with view option ,view the details for the feature	Failed	CSCwh01068

Global Network View with Network-Wide Path Insight Integration

Logical ID	Title	Description	Status	Defect ID
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.01	To Monitor the tunnel health using global network for individual site.	Monitoring for tunnel health for individual site under global network view	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.02	To view the overlay networks tunnels using geographic map location of sites.	Monitoring overlay network tunnels and location of sites using geographic map	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.03	To view the individual site health using with interactive icon	Viewing individual site health in Global topology view using interactive icon	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.04	To filter the tunnel health using advanced filter panel	Monitoring Tunnel health using advanced filter options	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.05	To view the tunnel health summary in topology panel	Monitoring the tunnel health summary in topology panel	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.06	To Monitor the Single site map by clicking on site from network hierarchy panel	Checking single site map by clicking on site from network hierarchy panel	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.07	To view the list of tunnels in tabular format using tunnel link	By using tunnel link, check able to view the list of tunnels in tabular format.	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.08	To view the global network view using time filter	Monitoring the Global Network View by using the time filter	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.09	To monitor the interactive chart with time slots under global network overview.	Monitoring the Global Network View by using the time filter	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.10	To change the time chart settings using Toggle switch	Monitoring the Global Network View by using the time filter	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.11	check the behavior of time change in the interactive chart by user interactions	Monitoring the time change in the interactive chart by user interactions	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.12	To monitor the summary of all devices for site with network hierarchy	Monitoring the summary of all devices for site with network hierarchy	Passed	

ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.13	To trace a route using NWPI tool	To create a new trace and view the route y using Nwpi tool.	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.14	To view the insights summary using NWPI tool	By using the nwpi tool open the insights summary.	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.15	To view the heatmap chart for site health using Network Hierarchy	In global network topology, to view the heatmap chart for the site health.	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.16	To analyze the traffic flow between the Dc and branch devices using NWPI.	By using trace route in nwpi tools, create a trace route between the DC and Branch devices.	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.17	To monitor the NWPI TOOLS using site topology device sidebar	By using site topology device sidebar check whether able to view the NWPI tools.	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.18	Check the tunnel performance by hovering over the tunnel link.	Checking the performance of tunnels by hovering over the tunnel links from vManage dashboard	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.19	To filter the site health using advanced filter panel	Applying Time filter from Global Network view from v-Manage dashboard	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.20	To view the Qos insight and App Performance insight in the NWPI Dashboard.	To view the Qos insight and App Performance insight in the NWPI Dashboard	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.21	To check able to delete the running trace	Check whether able to create and delete a running trace in NWPI	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.22	To check able to view application / event distribution in NWPI Dashboard	Check whether able to view event distribution in NWP	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.23	To check able to view event impact in NWPI	Check whether able to view event impact in NWPI	Passed	
ENJ. UX 2.0 Mon.20.12.1_17.12.1_ N.24	To create nwpi new trace in geographic view with grouping fields	Creating new trace in nwpi with geographic view by including grouping fields	Failed	CSCwf84274

vManage - Security Enhanced dashboard

Logical ID	Title	Description	Status	Defect ID
ENJ.Sec.20.12.1_17.12.1_N.01	To verify if pie chart and bar chart in the Firewall Rule Counter dashlet is displayed.	Verifying the Firewall Rule Counter Dashlet is displaying the Pie chart/Bar Graph.	Passed	
ENJ.Sec.20.12.1_17.12.1_N.02	To Verify the Top Rules filter Drop down, if the bar chart is displayed based on Firewall rule is Allowed/Dropped/Inspected.	Verifying the Top Rules filter Drop down is clickable & displaying the bar chart based on Firewall rule is Allowed/Dropped/Inspected.	Passed	
ENJ.Sec.20.12.1_17.12.1_N.03	To Verify if View Details displays the side bar with all the Rules in Firewall Section.	Verifying if the View Details at the bottom of the dashlet, can be viewed further details like the policy name rule is part of.	Passed	
ENJ.Sec.20.12.1_17.12.1_N.04	To Verify by clicking the device hits displays all the device information in Firewall Section.	Verifying to displays the details of the devices that got impacted, by clicking the “No of devices Hits”.	Failed	CSCwf76221
ENJ.Sec.20.12.1_17.12.1_N.05	To Verify if line chart in Intrusion Prevention dashlet is displayed.	Verify the Intrusion Prevention Dashlet is displaying the Line chart.	Passed	
ENJ.Sec.20.12.1_17.12.1_N.06	To Verify if View Details displays the high/low/medium risk entries for a given time entry in Intrusion Prevention.	Verifying if the View Details displays the high/low/medium risk entries for a given time entry in Intrusion Prevention.	Passed	
ENJ.Sec.20.12.1_17.12.1_N.07	To Verify by clicking the event count displays all the events, their occurrences and devices impacted count in Intrusion prevention.	Verifying by clicking the event count displays all the events, their occurrences and devices impacted count in Intrusion prevention.	Passed	

ENJ.Sec.20.12.1_17.12.1_N.08	To Verify by clicking the device hits, displays all the device information in Intrusion Prevention.	Verifying by clicking the device hits/impacted, displays all the device information in Intrusion Prevention. And by clicking the host name in device impacted table should redirect to Device 360 Page.	Passed	CSCwf37830
ENJ.Sec.20.12.1_17.12.1_N.09	To Verify if line chart in Advanced Malware Protection (AMP) dashlet is displayed.	Verifying the Advanced Malware Protection Dashlet is displaying the Line chart.	Passed	
ENJ.Sec.20.12.1_17.12.1_N.10	To Verify if View Details displays the Clean/Malicious/Unknown file counts Information in AMP.	Verifying if View Details Displays the Clean/Malicious/Unknown file counts information in Advanced Malware Protection.	Passed	
ENJ.Sec.20.12.1_17.12.1_N.11	To Verify the file count displays the name of all the files, their occurrences and devices impacted count in AMP.	Verifying the file count displays the details of name of all the files, their occurrences and devices impacted count, file reputation & file availability.	Passed	
ENJ.Sec.20.12.1_17.12.1_N.12	To Verify by clicking the device hits displays all the device information in AMP.	Verifying by clicking the device hits displays all the device information & Clicking on the Hostname in devices impacted table, will redirect to the Device 360 page in AMP.	Passed	
ENJ.Sec.20.12.1_17.12.1_N.13	To Verify the pie chart and bar chart in URL Filtering dashlet is displayed.	From vManage Security page, verify the pie chart and bar chart in URL Filtering dashlet is displayed.	Passed	CSCwf39120

ENJ.Sec.20.12.1_17.12.1_N.14	To Verify by clicking the Top URL Category Drop down filters the bar based on rule is Blocked/Allowed/Exempted in URL Filtering.	From the URL Filtering Dashlet, go to the Top URL Category, then check Drop down filters the bar based on rule is Blocked/Allowed/Exempted in URL Filtering.	Passed	
ENJ.Sec.20.12.1_17.12.1_N.15	To Verify if View Details displays the side bar with the URL Filtering category information.	By clicking of view details will display the URL category, Action and no of device accessed	Passed	
ENJ.Sec.20.12.1_17.12.1_N.16	To Verify by clicking the device hits displays all the device information in URL Filtering.	The device hits displays all the device information in URL Filtering. & also clicking on the Hostname in devices impacted table, will redirect to the Device 360 page	Failed	CSCwh01097
ENJ.Sec.20.12.1_17.12.1_N.17	To Verify if View details redirects to Monitor – Logs – Events page in Security Events dashlet is displayed.	Verifying by clicking on view details redirects to Monitor – Logs – Events page in Security Events dashlet is displayed	Passed	

Cisco Catalyst SD-WAN Remote Access Configuration in SSL-VPN Mode

Logical ID	Title	Description	Status	Defect ID
ENJ.SDRASSL.20.11.1_17.11.1_N01	Configure C8000v Router as a SD-WAN RA Headend router using vManage Config Group	Verify configuration group option to create remote access configuration	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N02	Configure a Enterprise CA server IP address and Verify with UX2.0 Config	Verify the Enterprise CA server	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N03	Configure a CA server IP address and Verify with CLI Config and manually enroll	Verify the Enterprise CA server using CLI and enroll Maually	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N04	Edit or modify AAA ISE as RADIUS Server in ux2.0 system profile	Verify the AAA ISE Radius server	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N05	Configure ISE as RADIUS Server and Verify with CLI Config	Verify the AAA ISE Radius server in CLI	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N06	Configure ISE server with Authentication and AuthoriZation policy	Verify the Authentication and Authorization policy for ISE Radius server	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N07	Create ipv4 IP Pool manually using CLI and verify not ipv6 option is not supported	Verify the IPv4 ip pool for sdra SSL using CLI	Passed	

ENJ.SDRASSL.20.11.1_17.11.1_N08	Configure SDRA Config Group with user Auth & Disable profile download	Verify the option User Authentication for Any connect EAP	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N09	Configure SDRA Config Group with user Auth & Enable profile download	Verify the option User Authentication and profile download for Any connect EAP	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N10	Configure AAA Policy & specify default policy name and password	Verify the AAA policy and set the default username and password	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N11	Configure AAA Policy & specify both user name and password with default values	Verify the AAA policy and set the both username and password with default values	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N12	Configure AAA Policy & Derive Global policy name and password	Verify the AAA policy and set the global policy name and password	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N13	Configure headend device using cli add-on template	Verify the headend device using cli add-on template	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N14	Disconnect session and check the stats and traffic	Verify disconnected session and check the stats and traffic	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N15	Configure Crypto ssl policy & profile using cli and verify	Verify Crypto ssl policy & profile using cli	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N16	Configure SDRA Virtual template using CLI	Verify the SDRA Virtual template using CLI	Passed	

ENJ.SDRASSL.20.11.1_17.11.1_N17	Configure SSL vpn and try to get the virutual access template in router and get the ip address in client machine from IP pool	Verify SSL vpn and try to get the virutual access template in router and get the ip address in client machine from IP pool	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N18	Configure SSL VPN and try to access http or https server	Verify SSL VPN and try to access http or https server		
ENJ.SDRASSL.20.11.1_17.11.1_N19	Configure AAA using CLI	Verify AAA using CLI	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N20	Configure SSL vpn and try to get the virutual access template in router and get the ip address in client machine from IP pool using CLI	Verify SSL vpn and try to get the virutual access template in router and get the ip address in client machine from IP pool using CLI	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N21	Advertise SDRA IP pool subnets into OMP as aggregate-only route in the service VPNs	Verify OMP as aggregate-only route in the service VPNs	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N22	Configure ACL to permit the client machine to get access to server	Verify ACL to permit the client machine to get access to server	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N23	Configure ACL to deny the client machine to get access to server	Verify ACL to deny the client machine to get access to server	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N24	Check user & Device Authentication is disabled and not support for the current SSL VPN	Verify user & Device Authentication is disabled and not support for the current SSL VPN	Passed	
ENJ.SDRASSL.20.11.1_17.11.1_N25	Check PSK option is disabled and not support for the current SSL VPN	Verify PSK option is disabled and not support for the current SSL VPN	Passed	

ENJ.SDRASSL.20.11.1_17.11.1_N26	Configure route set prefix and AAA Policy password (optional) extension in authorization	Verify route set prefix and AAA Policy password (optional) extension in authorization	Passed	

Symmetric Routing-Management Region-intent based hub-spoke-On-demand tunnels with TGW

Logical ID	Title	Description	Status	Defect ID
ENJ.MRF.20.12.1_17.12.1_N.01	Configure and redistribute omp translate-rib-metric in BGP address-family ipv4 unicast vrf and verify the results.	To redistribute omp translate-rib-metric into BGP and verify the routes, to test the LAN side functionality.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.02	Configure and redistribute omp translate-rib-metric in BGP address-family ipv6 unicast vrf and verify the results.	To redistribute omp translate-rib-metric into BGP and verify the ipv6 routes, to test the LAN side functionality.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.03	Configure and redistribute omp translate-rib-metric with route-map in BGP address-family ipv4 unicast vrf for particular ip prefixes.	To redistribute omp translate-rib-metric into BGP and verify the routes with route-map, to test the LAN side functionality.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.04	Configure and redistribute omp translate-rib-metric with route-map set as-path prepend as-path-list in BGP address-family ipv4 unicast vrf	To redistribute omp translate-rib-metric into BGP and verify the routes by prepending the AS path to test the LAN side functionality.	Passed	

ENJ.MRF.20.12.1_17.12.1_N.05	Configure and redistribute omp translate-rib-metric with route-map set as-path prepend as-path-list in BGP address-family ipv6 unicast vrf	To redistribute omp translate-rib-metric into BGP and verify the routes by prepending the AS path to test the LAN side functionality.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.06	Configure and to redistribute omp translate-rib-metric with route-map set metric in BGP address-family ipv4 unicast vrf	To redistribute omp translate-rib-metric into BGP and verify the routes by setting metric and to test the LAN side functionality.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.07	Configure and to redistribute omp translate-rib-metric with route-map set metric in BGP address-family ipv6 unicast vrf	To redistribute omp translate-rib-metric into BGP and verify the routes by setting metric and to test the LAN side functionality	Passed	
ENJ.MRF.20.12.1_17.12.1_N.08	Configure and to redistribute omp translate-rib-metric with route-map set local-preference in BGP address-family ipv4 unicast vrf and verify routes	To redistribute omp translate-rib-metric into BGP and verify the routes by setting local preference and to test the LAN side functionality	Passed	
ENJ.MRF.20.12.1_17.12.1_N.09	Configure and to redistribute omp translate-rib-metric with route-map set local-preference in BGP address-family ipv6 unicast vrf and verify routes	To redistribute omp translate-rib-metric into BGP and verify the routes by setting local preference and to test the LAN side functionality.	Passed	

ENJ.MRF.20.12.1_17.12.1_N.10	Configure and to redistribute omp translate-rib-metric in BGP address-family ipv4 unicast vrf using vManage Template push	Configure the redistribution of omp translateto BGP through vManage template	Passed	
ENJ.MRF.20.12.1_17.12.1_N.11	Configure and to redistribute omp translate-rib-metric under ospfv2 vrf process.	To configure and to redistribute omp translate-rib-metric under ospfv2 and verify the LAN functionality.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.12	Configure and to redistribute omp translate-rib-metric under ospfv3 address-family ipv4	To configure and to redistribute omp translate-rib-metric under ospfv3 and verify the LAN functionality.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.13	Configure and to redistribute omp translate-rib-metric under ospfv3 address-family ipv6	To configure and to redistribute omp translate-rib-metric under ospfv3 with Ipv6 and verify the LAN functionality.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.14	Configure gateway affinity preference on Cedge (access router in region 1) and check the logs	To configure the affinity preference on Cedge as 1 in the access region 1 without applying the filer knob in vsmart	Passed	
ENJ.MRF.20.12.1_17.12.1_N.15	Configure gateway affinity preference on Cedge (border router for region 1) and check the logs	Configure the affinity preference on the border router and check the preference and path	Passed	
ENJ.MRF.20.12.1_17.12.1_N.16	Remove gateway affinity preference on Cedge (both access router and border routers in the region 1) and verify the routes.	Remove the affinity preference on BR and ER and verify the logs.	Passed	

ENJ.MRF.20.12.1_17.12.1_N.17	Reload the vSmart and border router in region 1 and check the behaviour.	Reload the vSmart in BR1 and check the logs.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.18	Reload the vSmart and boder router in region 0 and check the behaviours.	Reload the vSmart in BR1 and check the logs.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.19	Configure the OMP on the border router to Shut/un-Shut and observe the behaviour.	Shut and unshut the access router in region 1 and check the logs.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.20	Configure the on-demand tunnel on access router with Transport gateway enabled in region 1.	Configure the tunnel on the access router with TGW in region 1 and verify the logs.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.21	Bring down BFD between Access router and the boder router and Transport gateway and check on-demand tunnel status in the region 1.	Bring down the bfd between access routers and the border router and check the logs.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.22	Configure the on-demand tunnel between access routers in same region with Transport gate way.	Configure the on-demand tunnel between access routers with the TGW border routers and verify logs.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.23	Clear the OMP routes on border routers and verify the omp routes in the access routers.	To test the behaviour after clearing the OMP routes in the area 0 core routers.	Passed	
ENJ.MRF.20.12.1_17.12.1_N.24	Configure Affinity preference-order-auto on ER,BR and verify the routes and path.	To verify the affinity preference auto behaviour	Passed	

ENJ.MRF.20.12.1_17.12.1_N.25	Configure and verify the symmetric routing with the Non MRF region and verify the routes	To verify the symmetric routing with the Non MRF region and verify the routes	Passed	
ENJ.MRF.20.12.1_17.12.1_N.26	Configure and verify per-vrf affinity on TGW for non MRF region to test the behavior	To verify per-vrf affinity on TGW for non MRF region to test the behavior	Passed	

Enabling MACsec using Cisco SD-WAN

Logical ID	Title	Description	Status	Defect ID
ENJ.MACSec_20.12.1_17.12.1_N.01	Configuring key chain in Service side Device	Verify after Key Chain config in Service Side Device	Passed	
ENJ.MACSec_20.12.1_17.12.1_N.02	Configure MKA PSK Key chain	Configure MKA PSK Key chain when the Device in is Autonomous Mode(P2P)	Passed	
ENJ.MACSec_20.12.1_17.12.1_N.03	Configure MKA PSK Key chain with lifetime options	Configure MKA PSK Key chain with lifetime options and Verfy	Passed	
ENJ.MACSec_20.12.1_17.12.1_N.04	Configure MKA PSK Key chain with cryptographic-alg options and Verify	Configure MKA PSK Key chain with cryptographic-alg options and Verify	Passed	
ENJ.MACSec_20.12.1_17.12.1_N.05	Verify after Delete PSK Key chain from device	Verify after Delete PSK Key chain from device and check its deleted or not	Passed	
ENJ.MACSec_20.12.1_17.12.1_N.06	Configure MKA PSK Key chain	Configure DIA Policy Config by CLI Template with MKA PSK Key chain and verify	Passed	
ENJ.MACSec_20.12.1_17.12.1_N.07	Configure MKA policy through the CLI template and verify	Configure MKA PSK Key chain with lifetime options and Verfy	Passed	
ENJ.MACSec_20.12.1_17.12.1_N.08	Configure Policy Parameters – SAK Rekey interval, conf-offset, cipher-suite	Configure Policy Parameters – SAK Rekey interval, conf-offset, cipher-suite and verify	Passed	

ENJMACSec_20.12.1_17.12.1_N.09	Delete MKA Policy and verify through the template	Delete MKA Policy and verify through the template	Passed	
ENJMACSec_20.12.1_17.12.1_N.10	MKA PSK Key Config in Service Interface and verify	MKA PSK Key Config in Service Interface and verify	Passed	
ENJMACSec_20.12.1_17.12.1_N.11	Configuring PSK on an interface and verify	Configuring PSK on an interface and verify	Passed	
ENJMACSec_20.12.1_17.12.1_N.12	Configure the fallback key on a Service interface	Configure the fallback key on a Service interface	Passed	
ENJMACSec_20.12.1_17.12.1_N.13	Configure MKA policy on an interface and verify	Configure MKA policy on an interface and verify	Passed	
ENJMACSec_20.12.1_17.12.1_N.14	Unconfigure All policy from an interface and verify	Unconfigure all policy from an interface and verify	Passed	
ENJMACSec_20.12.1_17.12.1_N.15	Unconfigure PSK from an interface and verify	Unconfigure PSK from an interface and verify	Passed	
ENJMACSec_20.12.1_17.12.1_N.16	Verify Configuring MACSEC over the interface	Verify Configuring MACSEC over the interface	Passed	
ENJMACSec_20.12.1_17.12.1_N.17	Verify MKA with destination mac multicast	Verify MKA with destination mac multicast	Passed	
ENJMACSec_20.12.1_17.12.1_N.18	Verify MKA with destination mac broadcast	Verify MKA with destination mac broadcast	Passed	
ENJMACSec_20.12.1_17.12.1_N.19	Verify Functionality after enabling macsec (PD cli) in interface	Verify Functionality after enabling macsec (PD cli) in interface	Passed	
ENJMACSec_20.12.1_17.12.1_N.20	Verify functionality with should/must-secure (PD cli)	Verify functionality with should/must-secure (PD cli)	Passed	

ENJ.MACSec_20.12.1_17.12.1_N21	Verify show clis for mka sessions, statistics for interface in Controller mode	Verify show clis for mka sessions, statistics for interface in Contrroller Mode	Passed	
ENJ.MACSec_20.12.1_17.12.1_N22	Verify show clis for global mka sessions, statistics	Verify show clis for global mka sessions, statistics in Autonomous mode	Passed	
ENJ.MACSec_20.12.1_17.12.1_N23	Send the traffic from Coexisting Macsec to non-macsec serviceside	Send the traffic from Coexisting Macsec to non-macsec serviceside	Passed	
ENJ.MACSec_20.12.1_17.12.1_N24	Configuring Macsec with NAT in Service side and verify	Configuring Macsec with NAT in Service side and verify	Passed	
ENJ.MACSec_20.12.1_17.12.1_N25	Configuring Macsec with Zone-Base firewall and Verify	Configuring Macsec with Zone-Base firewall and Verify	Passed	
ENJ.MACSec_20.12.1_17.12.1_N26	Configuring Mecsec On VRRP Interface and verify	Configuring Mecsec On VRRP Interface and verify	Passed	

IPv6 GRE-IPSEC Tunnels to Third party-Generic Integration

Logical ID	Title	Description	Status	Defect ID
ENJJPV6_GRE20.12.1_17.12.1_N01	Create ipv6 SVTI ipsec tunnel in service side vpn and verify	Verify ipv6 SVTI ipsec tunnel in service side vpn	Passed	
ENJJPV6_GRE20.12.1_17.12.1_N02	Create ipv6 GRE tunnel in service side vpn and verify	Verify ipv6 GRE tunnel in service side vpn	Passed	
ENJJPV6_GRE20.12.1_17.12.1_N03	Create ipv6 SVTI ipsec tunnel in service side vpn and connect another router	Verify ipv6 SVTI ipsec tunnel in service side vpn and connect another router	Passed	
ENJJPV6_GRE20.12.1_17.12.1_N04	Create ipv6 GRE tunnel in service side vpn and connect another router	Verify ipv6 GRE tunnel in service side vpn and connect another router	Passed	
ENJJPV6_GRE20.12.1_17.12.1_N05	Create Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o4 GRE/SVTI tunnel	Verify Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o4 GRE/SVTI tunnel	Passed	
ENJJPV6_GRE20.12.1_17.12.1_N06	Create Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o4 GRE/SVTI tunnel & withdraw route via vm3 on vm5	Verify Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o4 GRE/SVTI tunnel & withdraw route via vm3 on vm5	Passed	

ENJ.IPV6_GRE.20.12.1_17.12.1_N07	Create Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o4 GRE/SVTI tunnel & Wait for session come up and then unconfig tunnel pre-route mandatory	Verify Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o4 GRE/SVTI tunnel & Wait for session come up and then unconfig tunnel pre-route mandatory	Passed	
ENJ.IPV6_GRE.20.12.1_17.12.1_N08	Create Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o4 GRE/SVTI tunnel & withdraw route via vm3 on vm5 then unconfig tunnel pre-route mandatory	Verify Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o4 GRE/SVTI tunnel & withdraw route via vm3 on vm5 then unconfig tunnel pre-route mandatory	Passed	
ENJ.IPV6_GRE.20.12.1_17.12.1_N09	Create Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o4 GRE/SVTI tunnel & Config tunnel pre-route mandatory to Gi4	Verify Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o4 GRE/SVTI tunnel & Config tunnel pre-route mandatory to Gi4	Passed	
ENJ.IPV6_GRE.20.12.1_17.12.1_N10	Create Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o6 GRE/SVTI tunnel	Verify Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o6 GRE/SVTI tunnel	Passed	

ENJJPV6_GRE20.12.1_17.12.1_N11	Create Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o6 GRE/SVTI tunnel & withdraw route via vm3 on vm5	Verify Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o6 GRE/SVTI tunnel & withdraw route via vm3 on vm5	Passed	
ENJJPV6_GRE20.12.1_17.12.1_N12	Create Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o6 GRE/SVTI tunnel & Wait for session come up and then unconfig tunnel pre-route mandatory	Verify Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o6 GRE/SVTI tunnel & Wait for session come up and then unconfig tunnel pre-route mandatory	Passed	
ENJJPV6_GRE20.12.1_17.12.1_N13	Create Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o6 GRE/SVTI tunnel & withdraw route via vm3 on vm5 then unconfig tunnel pre-route mandatory	Verify Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o6 GRE/SVTI tunnel & withdraw route via vm3 on vm5 then unconfig tunnel pre-route mandatory	Passed	
ENJJPV6_GRE20.12.1_17.12.1_N14	Create Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o6 GRE/SVTI tunnel & Config tunnel pre-route mandatory to Gi4	Verify Tunnel pre-route mandatory configured on edge Router through Gig1 vpn0 for 6o6 GRE/SVTI tunnel & Config tunnel pre-route mandatory to Gi4	Passed	

ENJ.IPV6_GRE.20.12.1_17.12.1_N15	Create 6o4 GRE/ SVTI tunnel configuration and eBGP configuration could be populated via vManage CLI template	Verify 6o4 GRE/ SVTI tunnel configuration and eBGP configuration could be populated via vManage CLI template	Passed	
ENJ.IPV6_GRE.20.12.1_17.12.1_N16	Create 6o6 GRE/ SVTI tunnel configuration and eBGP configuration could be populated via vManage CLI template	Verify 6o6 GRE/ SVTI tunnel configuration and eBGP configuration could be populated via vManage CLI template	Passed	
ENJ.IPV6_GRE.20.12.1_17.12.1_N17	Create GRE 6o4 2 ECMP path Tunnel64 for ipv4	Verify GRE 6o4 2 ECMP path Tunnel64 for ipv4	Passed	
ENJ.IPV6_GRE.20.12.1_17.12.1_N18	Create GRE 6o6 2 ECMP path Tunnel66 for Ipv6	Verify GRE 6o6 2 ECMP path Tunnel66 for Ipv6	Passed	
ENJ.IPV6_GRE.20.12.1_17.12.1_N19	Create SVTI IPSEc 6o4 2 ECMP for IPv4	Verify SVTI IPSEc 6o4 2 ECMP for IPv4	Passed	
ENJ.IPV6_GRE.20.12.1_17.12.1_N20	Create SVTI ipsec 6o6 2 ECMP path Tunnel166 for IPv6	Verify SVTI ipsec 6o6 2 ECMP path Tunnel166 for IPv6	Passed	

Cat8K and ISR1K-Trustsec SDA-SDWAN Scale Measurement

Logical ID	Title	Description	Status	Defect ID
ENJ.TrustSec_20.12.1_17.12.1_N.01	Configuring Trustsec check the Traffic not going through LAN-to-WAN	Configuring Trustsec check the Traffic not going through LAN-to-WAN	Passed	
ENJ.TrustSec_20.12.1_17.12.1_N.02	Check if the route for Host is first present in the RIB or not	Check if the route for Host is first present in the RIB or not	Passed	
ENJ.TrustSec_20.12.1_17.12.1_N.03	Check OMP route if it is present in OMP database as well and advertised or not	Check OMP route if it is present in OMP database as well and advertised or not	Passed	
ENJ.TrustSec_20.12.1_17.12.1_N.04	Check if the route is present make sure it is in the forwarding layer (FMAN-RP/FP/CPP layer in that order).	Check if the route is present make sure it is in forwarding layer (FMAN-RP/FP/CPP layer in that order).	Passed	
ENJ.TrustSec_20.12.1_17.12.1_N.05	Check if the route is present MS/MR LISP system, and is being distributed properly to RIB or not	Check if the route is present MS/MR LISP system, and is being distributed properly to RIB or not	Passed	
ENJ.TrustSec_20.12.1_17.12.1_N.06	Check if the route is present in the routing protocol (OSPF/BGP) whichever is configured for that VRF interface or not	Check if the route is present in the routing protocol (OSPF/BGP) whichever is configured for that VRF interface or not	Passed	
ENJ.TrustSec_20.12.1_17.12.1_N.07	Check the Autonomous mode scaling after config by Max Unidirectional IPv4 SXP Connections	Check the Autonomous mode scaling after config by Max Unidirectional IPv4 SXP Connections	Passed	

ENJ.TrustSec_20.12.1_17.12.1_N.08	Check the Autonomous mode CPU & SXP Core Memory Utilisation scaling after config by Max Unidirectional IPv4 SXP Connections	Check the Autonomous mode CPU & SXP Core Memory Utilisation scaling after config by Max Unidirectional IPv4 SXP Connections	Passed	
ENJ.TrustSec_20.12.1_17.12.1_N.09	Check the Autonomous mode scaling after config by Bi-directional IPv4 SXP connections	Check the Autonomous mode scaling after config by Bi-directional IPv4 SXP connections	Passed	
ENJ.TrustSec_20.12.1_17.12.1_N.10	Check the Autonomous mode scaling after config by IPv4 SGT Bindings	Check the Autonomous mode scaling after config by IPv4 SGT Bindings	Passed	
ENJ.TrustSec_20.12.1_17.12.1_N.11	Check the Autonomous mode scaling after config by IPv6 SGT Bindings	Check the Autonomous mode scaling after config by IPv6 SGT Bindings	Passed	
ENJ.TrustSec_20.12.1_17.12.1_N.12	Check the Controller mode scaling after config by IPv4 SGT Bindings	Check the Controller mode scaling after config by IPv4 SGT Bindings	Passed	
ENJ.TrustSec_20.12.1_17.12.1_N.13	Check the Controller mode scaling after config by IPv6 SGT Bindings	Check the Controller mode scaling after config by IPv6 SGT Bindings	Passed	
ENJ.TrustSec_20.12.1_17.12.1_N.14	Check the SG ACEs scaling when the Device is in Controller modes	Check the SG ACEs scaling when the Device is in Controller modes	Passed	

ENJ.TrustSec_20.12.1_17.12.1_N.15	Check the Controller mode CPU & SXP Core Memory Utilisation scaling after config by Max Unidirectional IPv4 SXP Connections	Check the Controller mode CPU & SXP Core Memory Utilisation scaling after config by Max Unidirectional IPv4 SXP Connections	Passed	
ENJ.TrustSec_20.12.1_17.12.1_N.16	Configuring SGT/DGT Policies by cli and check the Memory Utilization	Configuring SGT/DGT Policies by cli and check the Memory Utilization	Passed	

Improved Brownout detection and Traffic steering

Logical ID	Title	Description	Status	Defect ID
ENJ.LPF.20.12.1_17.12.1_N.01	Verify SLA dampening when IPSEC tunnel meets SLA.	To check the SLA damping behaviour.	Passed	
ENJ.LPF.20.12.1_17.12.1_N.02	Verify EPFR loss causes SLA change for IPSEC tunnel.	To verify EPFR loss causes SLA changes	Passed	
ENJ.LPF.20.12.1_17.12.1_N.03	Verify EPFR config push using vManage on DUT using CLI add-on Templets.	Create a feature template and push the config to DUT	Passed	
ENJ.LPF.20.12.1_17.12.1_N.04	Verify EPFR config push using vManage on DUT using CLI Templets.	Create a cli template and push the config to DUT	Passed	
ENJ.LPF.20.12.1_17.12.1_N.05	To Verify EPFR WAN loss causes SLA change and switchover.	To verify the SLA breach.	Passed	
ENJ.LPF.20.12.1_17.12.1_N.06	Enable Epfr on cEdge and verify if expected logs are displayed.	To verify the SLA breach. With logging	Passed	
ENJ.LPF.20.12.1_17.12.1_N.07	Configure and verify Epfr with 5 SLA classes and verify the behavior.	To configure max 5 SLA classes without app-probe classes	Passed	
ENJ.LPF.20.12.1_17.12.1_N.08	Configure and verify epfr with aggressive timers and check the behavior.	Configure the aggressive mode with poll interval 10s and multiplier 5	Passed	
ENJ.LPF.20.12.1_17.12.1_N.09	Configure and verify epfr with moderate timers and check the behavior.	Configure the moderate mode with poll interval 20s and multiplier 5.	Passed	

ENJLPF20.12.1_17.12.1_N.10	Configure and verify epfr with aggressive and moderate timers and check the behavior.	Configure the moderate and aggressive mode	Passed	
ENJLPF20.12.1_17.12.1_N.11	Configure and verify epfr with dampening timers.	Configure and verify the EPFR with dampining timers and verify logs	Passed	
ENJLPF20.12.1_17.12.1_N.12	To change the system ip of the DUT and observe the behavior.	To change the system ip and observe the logs	Passed	
ENJLPF20.12.1_17.12.1_N.13	Shut and unshut the WAN Interface and verify the behavior of the tunnel when the traffic is pumped.	Test by shutting and unshutting the WAN Interface and check the behaviour.	Passed	
ENJLPF20.12.1_17.12.1_N.14	Verify epfr measurements when cEdge is reloaded and monitor the behavior with logs.	Reload the Cedge and observe the logs.	Passed	
ENJLPF20.12.1_17.12.1_N.15	To configure the adaptive qos for the sla class and check the WAN Loss	Monitoring the WAN LOSS Using the sla class.	Passed	

Routing vManage base automation for Autonomous mode

Logical ID	Title	Description	Status	Defect ID
ENJ.Auton.20.12.1_17.12.1_N01	To Verify installed image detail via vManage GUI.	To verify the installation image details	Passed	
ENJ.Auton.20.12.1_17.12.1_N02	Configuring a C8K Router to establish secure connection in Autonomous Mode.	By using configuration c8k router establish the secure connections in non controlled mode	Passed	
ENJ.Auton.20.12.1_17.12.1_N03	User MUST be able to SSH to C8K device from vManage.	check and verify the SSH from the vmanage in autonomous mode	Passed	
ENJ.Auton.20.12.1_17.12.1_N04	User MUST be able to ping on a C8K device from vManage.	check and verify the ping from the vmanage in autonomous mode	Passed	
ENJ.Auton.20.12.1_17.12.1_N05	User MUST be able to do traceroute C8K on a device from vManage.	check and verfy the traceroute of device from vmanage	Passed	
ENJ.Auton.20.12.1_17.12.1_N06	User MUST be able to retrieve logs, core-file, admin-tech for C8K devices from vManage.	checa and verify the retrive logs and admin logs ,core file in no sdwan devices	Passed	
ENJ.Auton.20.12.1_17.12.1_N07	Verify alarms generation and notification to vManage in autonomous mode.	Verify alarms generation and notification to vManage in autonomous mode.	Passed	
ENJ.Auton.20.12.1_17.12.1_N08	Verify event notification to vManage in autonomous mode.	Verify event notification to vManage in autonomous mode.	Passed	
ENJ.Auton.20.12.1_17.12.1_N09	Verify installed image detail via vManage.	check and Verify installed image detail via vManage.	Passed	

ENJ.Auton.20.12.1_17.12.1_N10	Verify the behavior of a router by Disabling & Enabling Controller-Managed.	check and Verify the behavior of a router by Disabling & Enabling Controller-Managed.	Passed	
ENJ.Auton.20.12.1_17.12.1_N11	Configuring a C8KV Router to establish secure connection in Autonomous Mode	By using Configuring a C8KV Router to establish secure connection in Autonomous Mode	Passed	
ENJ.Auton.20.12.1_17.12.1_N12	User MUST be able to SSH to C8KV device from vManage	heck the User MUST be able to SSH to C8KV device from vManage	Passed	
ENJ.Auton.20.12.1_17.12.1_N13	User MUST be able to ping on a C8KV device from vManage.	Check the User MUST be able to ping on a C8KV device from vManage.	Passed	
ENJ.Auton.20.12.1_17.12.1_N14	User MUST be able to do traceroute C8KV on a device from vManage.	Check the User MUST be able to do traceroute C8KV on a device from vManage.	Passed	
ENJ.Auton.20.12.1_17.12.1_N15	User MUST be able to retrieve logs, core-file, admin-tech for C8KV devices from vManage.	Check the User MUST be able to retrieve logs, core-file, admin-tech for C8KV devices from vManage.	Passed	
ENJ.Auton.20.12.1_17.12.1_N16	User MUST be able to retrieve logs, core-file, admin-tech for C8KV devices from CLI.	Check the User MUST be able to retrieve logs, core-file, admin-tech for C8KV devices from CLI.	Passed	
ENJ.Auton.20.12.1_17.12.1_N17	To Verify Reachability & Control Connections with the Wan Interface.	To Verify Reachability & Control Connections with the Wan Interface.	Passed	

ENJ.Auton.20.12.1_17.12.1_N18	To Verify Reachability & Control Connections after Flapping the Wan Interface	To Verify Reachability & Control Connections after Flapping the Wan Interface	Passed	
ENJ.Auton.20.12.1_17.12.1_N19	To Verify control connections with vManage comes up after rebooting the router.	To Verify control connections with vManage comes up after rebooting the router.	Passed	
ENJ.Auton.20.12.1_17.12.1_N20	To Verify control connections should go down after invalidating router in vManage GUI.	To Verify control connections should go down after invalidating router in vManage GUI.	Passed	
ENJ.Auton.20.12.1_17.12.1_N21	To Verify control connections should come up after validating router in vManage GUI.	To Verify control connections should come up after validating router in vManage GUI.	Passed	

Sr cfd

Logical ID	Tittle	Description	Status	Defect ID
ENJ.SRCFD.20.12.1_17.12.1_N.01	Verify the Fan Module information is accurately showing in vManage for C8500 Platform	The Fan Module Information should be accurately shown in the vManage GUI.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.02	Verify the Fan Module information is accurately showing in vManage for C8300 Platform	The Fan Module Information should be accurately shown in the vManage GUI.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.03	Verify the Fan Module information is accurately showing in vManage for C8200 Platform.	The Fan Module Information should be accurately shown in the vManage GUI.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.04	Verify the Fan Module information is accurately showing in vManage for ISR4461 Platform	The Fan Module Information should be accurately shown in the vManage GUI.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.05	Configure & Verify Service Timestamps through CLI on C8500 Platform.	Configure “Service Timestamps” through CLI & verify whether it can be configured or not.		
ENJ.SRCFD.20.12.1_17.12.1_N.06	Configure & Verify Service Timestamps through CLI on C8300 Platform.	Configure “Service Timestamps” through CLI & verify whether it can be configured or not.	Passed	

ENJ.SRCFD.20.12.1_17.12.1_N.07	Configure & Verify Service Timestamps through CLI on C8200 Platform.	Configure “Service Timestamps” through CLI & verify whether it can be configured or not.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.08	Configure & Verify Service Timestamps through CLI on C8KV Platform.	Configure “Service Timestamps” through CLI & verify whether it can be configured or not.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.09	Configure & Verify Service Timestamps through CLI on ISR4461 Platform	Configure “Service Timestamps” through CLI & verify whether it can be configured or not.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.010	Configure & Push Service Timestamps through CLI Add on template for C8500 Platform	Configure “Service Timestamps” through CLI Addon Template & verify whether it pushed or not	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.011	Configure & Push Service Timestamps through CLI Add on template for C8300 Platform.	Configure “Service Timestamps” through CLI Addon Template & verify whether it pushed or not.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.012	Configure & Push Service Timestamps through CLI Add on template for C8200 Platform.	Configure “Service Timestamps” through CLI Addon Template & verify whether it pushed or not.	Passed	

ENJ.SRCFD.20.12.1_17.12.1_N.013	Configure & Push Service Timestamps through CLI Add on template for C8KV Platform.	Configure “Service Timestamps” through CLI Addon Template & verify whether it pushed or not.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.014	Configure & Push Service Timestamps through CLI Add on template for ISR4461 Platform.	Configure “Service Timestamps” through CLI Addon Template & verify whether it pushed or not.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.015	Check Service Timestamps are reflected in Both Running-Config for C8500 Platform.	Configure “Service Timestamps” & verify It is reflected in Running-Config.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.016	Check Service Timestamps are reflected in Both Running-Config for C8300 Platform	Configure “Service Timestamps” & verify It is reflected in Running-Config.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.017	Configure & Push Service Timestamps through CLI Add on template for C8200 Platform.	Configure “Service Timestamps” & verify It is reflected in Running-Config.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.018	Configure & Push Service Timestamps through CLI Add on template for C8KV Platform.	Configure “Service Timestamps” & verify It is reflected in Running-Config.	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.019	Configure & Push Service Timestamps through CLI Add on template for ISR4461 Platform.	Configure “Service Timestamps” & verify It is reflected in Running-Config.	Passed	

ENJ.SRCFD.20.12.1_17.12.1_N.020	Configure the dual endpoint tracker with DNS server using CLI	By configure the dual endpoint tracker with DNS server using CLI	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.021	Configure the Multiple DNS Server in single endpoint tracker	By Configure the Multiple DNS Server in single endpoint tracker	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.022	Configure the ip address and DNS server with endpoint tracker	By Configure the ip address and DNS server with endpoint tracker	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.023	Check and verify the tracker status with first configured DNS Server and keeps query of Second DNS Server	By the tracker status with first configured DNS Server and keeps query of Second DNS Server	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.024	Check and verify the DUAL DNS server even the Query is failing	By the DUAL DNS server even the Query is failing	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.025	Configure SNMP with Encrypted Strings Using CLI Templates	By the SNMP with Encrypted Strings Using CLI Templates	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.026	Configure and enable SNMP notifications and check the memory leak using CLI	By the enable SNMP notifications and check the memory leak using CLI	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.027	Configure and Disable SNMP Traps and check the memory leak using CLI	By the Configure and Disable SNMP Traps and check the memory leak using CLI	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.028	Configure SNMP on Cisco IOS XE SD-WAN Devices Using CLI and check the memory leak	By using SNMP on Cisco IOS XE SD-WAN Devices Using CLI and check the memory leak	Passed	

ENJ.SRCFD.20.12.1_17.12.1_N.029	Check and Verify the memory Leak due to SNMP configuration after Remove	By using the memory Leak due to SNMP configuration after Remove	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.030	Configuring the device with cli template check the community-List in ISR router	By using the device with cli template check the community-List in ISR router	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.031	Configure and push the CLI template in Cat router	By using Configure and push the CLI template in Cat router	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.032	Check and verify the template once detached and again attached	By using Check and verify the template once detached and again attached	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.033	Configure and verify to push the cli template with and without community-list	By using the device with cli template check the community-List in ISR router	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.034	Configure and verify the physical interface over a loopback tunnel	By using Configure and verify the physical interface over a loopback tunnel	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.035	Configure the loopback interface with public address check the Reachability for DNS Server	By using Configure the loopback interface with public address check the Reachability for DNS Server	Passed	
ENJ.SRCFD.20.12.1_17.12.1_N.036	Verify and check the physical interface for resolving the vbonds hostname and not the loopback.	By using Verification and check the physical interface for resolving the vbonds hostname and not the loopback.	Passed	

Regression Features

- NAT, on page 56
- DIA, on page 60
- AAR and VPN Segmentation, on page 62
- TLOC, on page 65
- Path MTU, on page 67
- Vmanage UI, on page 69
- SD-AVC, on page 71
- SDRA, on page 72
- QoS, on page 74
- Adhoc, on page 77

NAT

Logical ID	Title	Status	Defect ID
ENJ.NAT.20.12.1_17.12.1_N01	To configure the Service side outside dynamic NAT with centralized data policy.	Passed	
ENJ.NAT.20.12.1_17.12.1_N02	To configure the Service side outside dynamic NAT overload with data policy.	Passed	
ENJ.NAT.20.12.1_17.12.1_N03	To configure the inside static NAT using an Inside Nat pool using centralized policy.	Passed	
ENJ.NAT.20.12.1_17.12.1_N04	To configure the static inside NAT and static outside Nat mapped inside Nat address pool	Passed	
ENJ.NAT.20.12.1_17.12.1_N05	To configure a service side PAT port forwarding with inside tcp traffic(http-80) via CLI.	Passed	
ENJ.NAT.20.12.1_17.12.1_N06	To configure a service side static Nat port forwarding with inside tcp traffic(telnet-23) via CLI.	Passed	
ENJ.NAT.20.12.1_17.12.1_N07	To configure the intra vpn service side Nat and generate the traffic and check the translation.	Passed	
ENJ.NAT.20.12.1_17.12.1_N08	To configure the service side conditional static Nat with data policy using CLI.	Passed	
ENJ.NAT.20.12.1_17.12.1_N09	To configure the service side conditional Dynamic Nat with data policy using CLI.	Passed	
ENJ.NAT.20.12.1_17.12.1_N10	To configure the service side Network Nat with data policy using CLI.	Passed	

ENJ.NAT.20.12.1_17.12.1_N11	To configure the service side static Nat object tracker with Data policy using cli.	Passed	
ENJ.NAT.20.12.1_17.12.1_N12	To configure the service side static Nat object tracker with Data policy using cli addon Template	Passed	
ENJ.NAT.20.12.1_17.12.1_N13	To configure the intra vpn service side Nat and generate the traffic using cli add on template	Passed	
ENJ.NAT.20.12.1_17.12.1_N14	To configure the service side conditional static Nat with matched and unmatched data policy and check the translation.	Passed	
ENJ.NAT.20.12.1_17.12.1_N15	To configure the service side static NAT using feature template and check the Nat translation	Passed	
ENJ.NAT.20.12.1_17.12.1_N16	To configure Source Port Preservation for DIA Interface Overload Using a CLI Template.	Passed	
ENJ.NAT.20.12.1_17.12.1_N17	To configure the Source Port Preservation for DIA Pool Overload Using a CLI Template.	Passed	
ENJ.NAT.20.12.1_17.12.1_N18	To configure the NAT DIA DUAL Tracker (Boolean OR) and the check the translation and tracker status.	Passed	
ENJ.NAT.20.12.1_17.12.1_N19	To configure the inside static NAT using an Inside Nat pool WITHOUT using centralized policy.	Passed	
ENJ.NAT.20.12.1_17.12.1_N20	To configure the service side static Nat object tracker with Data policy and check the behaviour of NAT Translation.	Passed	

ENJ.NAT.20.12.1_17.12.1_N21	To configure the NAT DIA Route using CLI and check the translation.	Passed	
ENJ.NAT.20.12.1_17.12.1_N22	To configure the NAT Route advertisements through OMP using the CLI and verify the translation.	Passed	
ENJ.NAT.20.12.1_17.12.1_N23	To configure the Dialler interface with NAT DIA and check the behaviour of NAT Translation.	Passed	
ENJ.NAT.20.12.1_17.12.1_N24	To configure the NAT DIA Static NAT Mapping with HSRP and check the behaviour of NAT Translation.	Passed	
ENJ.NAT.20.12.1_17.12.1_N25	To configure the ALG With NAT DIA for TFTP Protocol and check the behaviour of NAT Translation.	Passed	
ENJ.NAT.20.12.1_17.12.1_N26	To configure the port forwarding with NAT DIA Using a CLI Template and check the behaviour of NAT Translation.	Passed	
ENJ.NAT.20.12.1_17.12.1_N27	To Configure Destination Nat with DIA interface overload.	Passed	
ENJ.NAT.20.12.1_17.12.1_N28	To configure the NAT DIA DUAL Tracker (Boolean AND) and the check the translation and tracker status	Passed	
ENJ.NAT.20.12.1_17.12.1_N29	To configure the service side Dynamic NAT Inside (NAT Pool) + Static Port Forwarding only and check the behaviour of NAT Translation.	Passed	

ENJ.NAT.20.12.1_17.12.1_N30	To configure a dual destination with a dual source in conditional static NAT using data policy	Passed	

DIA

Logical ID	Title	Status	Defect ID
ENJ.DIA.20.12.1_17.12.1_N01	DIA Tracker status with DIA threshold configured with its maximum/minimum range value	Passed	
ENJ.DIA.20.12.1_17.12.1_N02	Dual Endpoint DIA in tracking group with Boolean OR operation on cisco IOS XE SD-Wan Device	Passed	
ENJ.DIA.20.12.1_17.12.1_N03	Configure the dual endpoint DIA with DNS server using CLI	Passed	
ENJ.DIA.20.12.1_17.12.1_N04	Configure the Multiple DNS Server in single endpoint DIA	Passed	
ENJ.DIA.20.12.1_17.12.1_N05	Configure the ip address and DNS server with endpoint DIA	Passed	
ENJ.DIA.20.12.1_17.12.1_N06	Check and verify the Tracker status with first configured DNS Server and keeps query of Second DNS Server	Passed	
ENJ.DIA.20.12.1_17.12.1_N07	Check and verify the DUAL DNS server even the Query is failing	Passed	
ENJ.DIA.20.12.1_17.12.1_N08	Dual Endpoint Support For interface Status tracking with on cisco IOS XE SD-Wan Device	Passed	
ENJ.DIA.20.12.1_17.12.1_N09	DIA Dual endpoint Tracking for interface in tracking Group by Vmanage	Passed	
ENJ.DIA.20.12.1_17.12.1_N10	Dual Endpoint DIA in tracking group with Boolean OR operation on cisco IOS XE SD-Wan Device	Passed	

ENJ.DIA.20.12.1_17.12.1_N11	DIA tracking with Dual Endpoint in DIA group by using Boolean AND operation	Passed	
ENJ.DIA.20.12.1_17.12.1_N12	DIA Dual endpoint DIA combination of DNS and DNS with AND operation by CLI	Passed	
ENJ.DIA.20.12.1_17.12.1_N13	DIA Dual endpoint DIA combination of IP and IP with OR operation by CLI	Passed	
ENJ.DIA.20.12.1_17.12.1_N14	DIA DIA for Track the endpoint With Internet transport link.	Passed	
ENJ.DIA.20.12.1_17.12.1_N15	DIA Dual endpoint DIA combination of DNS and IP with AND operation by CLI	Passed	
ENJ.DIA.20.12.1_17.12.1_N16	DIA Dual endpoint DIA combination of DNS and IP with OR operation by CLI	Passed	
ENJ.DIA.20.12.1_17.12.1_N17	DIA tracking with Dual Endpoint in DIA group by using Boolean AND operation by Vmanage	Passed	
ENJ.DIA.20.12.1_17.12.1_N18	DIA Dual endpoint DIA combination of DNS and DNS with AND operation by Vmanage	Passed	
ENJ.DIA.20.12.1_17.12.1_N19	DIA Dual endpoint DIA combination of DNS and DNS with OR operation by CLI	Passed	
ENJ.DIA.20.12.1_17.12.1_N20	DIA Dual endpoint DIA combination of IP and IP with OR operation by CLI	Passed	

AAR and VPN Segmentation

Logical ID	Title	Status	Defect ID
ENJ.VPN.20.12.1_17.12.1_N01	Configure VRF Segmentation Using the CLI (VRF100 VRF200)	Passed	
ENJ.VPN.20.12.1_17.12.1_N02	To configure BGP Service side to WAN Edge for VRF 100	Passed	
ENJ.VPN.20.12.1_17.12.1_N03	To configure OSPF Service side to WAN Edge for VRF 100	Passed	
ENJ.VPN.20.12.1_17.12.1_N04	To configure EIGRP Service side to WAN Edge for VRF 100	Passed	
ENJ.VPN.20.12.1_17.12.1_N05	Basic Policy with Custom Application	Passed	
ENJ.VPN.20.12.1_17.12.1_N06	Policy with Custom Application with Server name, IP	Passed	CSCwf36616
ENJ.VPN.20.12.1_17.12.1_N07	Policy with Custom Application with specified source IP and Port	Passed	
ENJ.VPN.20.12.1_17.12.1_N08	Policy with Custom Application with specified Server name and Ports	Passed	
ENJ.VPN.20.12.1_17.12.1_N09	Policy with Custom Application with specified source Ports and transport protocol(TCP/UDP)	Passed	
ENJ.VPN.20.12.1_17.12.1_N10	Color Preference and Count with Custom Application	Passed	
ENJ.VPN.20.12.1_17.12.1_N11	SLA low-loss low-latency Policy with Custom Application	Passed	
ENJ.VPN.20.12.1_17.12.1_N12	SLA low-loss high-latency Policy with Custom Application	Passed	

ENJ.VPN.20.12.1_17.12.1_N13	SLA high-loss high-latency Policy with Custom Application.	Passed	
ENJ.VPN.20.12.1_17.12.1_N14	Policy with Destination Data Prefix rule using vManage	Passed	CSCwf22638
ENJ.VPN.20.12.1_17.12.1_N15	Policy with Destination port rule using vManage	Passed	
ENJ.VPN.20.12.1_17.12.1_N16	Policy with Protocol rule using vManage	Passed	
ENJ.VPN.20.12.1_17.12.1_N17	Policy with Source Data Prefix rule using vManage	Passed	CSCwf36632
ENJ.VPN.20.12.1_17.12.1_N18	Policy with Source Port rule using vManage	Passed	
ENJ.VPN.20.12.1_17.12.1_N19	Policy with Destination port rule using CLI	Passed	
ENJ.VPN.20.12.1_17.12.1_N20	To Configure Cflowd Traffic Flow Monitoring Using the CLI	Passed	
ENJ.VPN.20.12.1_17.12.1_N21	To Configure Cflowd Traffic Flow Monitoring with ipv4-record using the CLI	Passed	
ENJ.VPN.20.12.1_17.12.1_N22	To Configure Cflowd Traffic Flow Monitoring Using vManage	Passed	
ENJ.VPN.20.12.1_17.12.1_N23	To Configure Cflowd Traffic Flow Monitoring with ipv4-records Using vManage	Passed	
ENJ.VPN.20.12.1_17.12.1_N24	Basic Policy to drop and use counter for a DPI application family using vmanage	Passed	
ENJ.VPN.20.12.1_17.12.1_N25	Basic Policy to accept and use counter for a DPI application using vManage	Passed	
ENJ.VPN.20.12.1_17.12.1_N26	Policy to forward to a Next hop for the application family using vManage	Passed	

ENJ.VPN.20.12.1_17.12.1_N27	Policy to forward to a TLOC colour for the application family with failover using vmanage	Passed	
ENJ.VPN.20.12.1_17.12.1_N28	Policy to forward to a TLOC color for the application family without failover using vManage	Passed	
ENJ.VPN.20.12.1_17.12.1_N29	Basic Policy to drop and use counter for a DPI application family using CLI	Passed	
ENJ.VPN.20.12.1_17.12.1_N30	Basic Policy to accept and use counter for a DPI application using CLI	Passed	

TLOC

Logical ID	Title	Status	Defect ID
ENJ.TLOC.20.12.1_17.12.1_N.01	Enable Ipv4 tloc extn for the Physical interface	Passed	
ENJ.TLOC.20.12.1_17.12.1_N.02	Disable ipv4 tloc extn for the Physical interface	Passed	
ENJ.TLOC.20.12.1_17.12.1_N.03	Config ipv4 tloc ext for the physical interface using vManage CLI template	Passed	
ENJ.TLOC.20.12.1_17.12.1_N.04	Enable ipv4 tloc extn for the sub interface	Passed	
ENJ.TLOC.20.12.1_17.12.1_N.05	Disable ipv4 tloc extn for the sub interface	Passed	
ENJ.TLOC.20.12.1_17.12.1_N.06	Config ipv4 tloc ext for the physical sub interface using vManage CLI template	Passed	
ENJ.TLOC.20.12.1_17.12.1_N.07	Enable ipv4 tloc extn for the loopback interface for extended wan circuits.	Passed	
ENJ.TLOC.20.12.1_17.12.1_N.08	Disable ipv4 tloc extn for the loopback interface for extended wan circuits	Passed	
ENJ.TLOC.20.12.1_17.12.1_N.09	Config ipv4 tloc ext for the Loopback interface using vManage CLI template	Passed	
ENJ.TLOC.20.12.1_17.12.1_N.10	Verify NAT for the physical sub-interface	Passed	
ENJ.TLOC.20.12.1_17.12.1_N.11	Check ipv4 tloc extn is advertise in OMP routes	Passed	
ENJ.TLOC.20.12.1_17.12.1_N.12	Check that dual sub interface is having ipv4 tloc extn	Passed	
ENJ.TLOC.20.12.1_17.12.1_N.13	Verify Implicit IPv4 ACL on TLOC tunnel interface	Passed	
ENJ.TLOC.20.12.1_17.12.1_N.14	Verify NAT for the Loopback Interface	Passed	

ENJ.TLOC.20.12.1_17.12.1_N.15	To create and verify ipv4 endpoint-tracker for physical interface	Passed	

Path MTU

Logical ID	Title	Status	Defect ID
ENJ.PMTU.20.12.1_17.12.1_N.01	To Branch 1 to DC with path mtu size 1496 and size 1496	Passed	
ENJ.PMTU.20.12.1_17.12.1_N.02	To Branch 1 to DC with path mtu size 1256 and size 128	Passed	
ENJ.PMTU.20.12.1_17.12.1_N.03	To Branch 1 to DC with path mtu size 1500 and size 1700 with DF=1	Passed	
ENJ.PMTU.20.12.1_17.12.1_N.04	To Branch 1 to DC with path mtu size 1496 and size 1900 with DF=1	Passed	
ENJ.PMTU.20.12.1_17.12.1_N.05	To Branch 1 to DC with path mtu size 128 and size 1250 with DF=1	Passed	
ENJ.PMTU.20.12.1_17.12.1_N.06	To Branch 1 to DC with path mtu size 1500 and size 1024	Passed	
ENJ.PMTU.20.12.1_17.12.1_N.07	To Branch 1 to DC with path mtu size 900 and size 4096	Passed	
ENJ.PMTU.20.12.1_17.12.1_N.08	To Branch 1 to DC with path mtu size 1496 and size 1450	Passed	
ENJ.PMTU.20.12.1_17.12.1_N.09	To Branch 1 to DC with path mtu size 1500 and size 1456 with DF=1	Passed	
ENJ.PMTU.20.12.1_17.12.1_N.10	Enable PMTU discovery on BFD Tunnel Interface from Branch 1 to DC	Passed	
ENJ.PMTU.20.12.1_17.12.1_N.11	Disable PMTU discovery on BFD Tunnel Interface from Branch 1 to DC	Passed	
ENJ.PMTU.20.12.1_17.12.1_N.12	Enable PMTU discovery on Service side LAN interface in Branch 1 vrf 100	Passed	

ENJ.PMTU.20.12.1_17.12.1_N.13	Enable PMTU discovery on Service side LAN interface in DC vrf 200	Passed	
ENJ.PMTU.20.12.1_17.12.1_N.14	Enable PMTU discovery on Service side LAN interface b/w service router in Branch1 vrf 100	Passed	
ENJ.PMTU.20.12.1_17.12.1_N.15	Enable PMTU discovery on Service side LAN interface b/w service switch in Branch1 vrf 100	Passed	

Vmanage UI

Logical ID	Title	Status	Defect ID
ENJ.VManageUI.20.12.1-_17.12.1_N.01	Check the Feature template working or not in daily build	Failed	CSCwf67086
ENJ.VManageUI.20.12.1-_17.12.1_N.02	Try to Edit and view the Root Certificate Button at Administration Setting in Vmanage	Failed	CSCwf42521
ENJ.VManageUI.20.12.1-_17.12.1_N.03	Check the Feature template working or not in daily build	Failed	CSCwf88277
ENJ.VManageUI.20.12.1-_17.12.1_N.04	policy still exists even after successful deletion	Failed	CSCwf75918
ENJ.VManageUI.20.12.1-_17.12.1_N.05	To verify navigating to Security Policies/Profiles Under Configurations.	Failed	CSCwf22563
ENJ.VManageUI.20.12.1-_17.12.1_N.06	Log into vManage and navigate to Monitor > Logs > Alarms page.	Failed	CSCwf32045
ENJ.VManageUI.20.12.1-_17.12.1_N.07	Try to choose/unchoose options under gear settings in Policy groups.	Failed	CSCwf40817
ENJ.VManageUI.20.12.1-_17.12.1_N.08	Try to navigate into group of intrests and create some policies	Failed	CSCwf40878
ENJ.VManageUI.20.12.1-_17.12.1_N.09	Try to connect a USB Stick to the Edge Router and verify it vManage.	Failed	CSCwf40903
ENJ.VManageUI.20.12.1-_17.12.1_N.10	Try to navigate into Cloud OnRamp for SaaS and create Application and policy.	Passed	CSCwf43710
ENJ.VManageUI.20.12.1-_17.12.1_N.11	Try to Create a Empty Topology under Configuration.	Failed	CSCwf44757
ENJ.VManageUI.20.12.1-_17.12.1_N.12	Create a topology under confiugration and try to add spoke group to it.	Failed	CSCwf44809

ENJ.VManageUI.20.12.1-_17.12.1_N.13	Navigate to Administration > Root CA Management and modify Root CA.	Passed	CSCwf50047
ENJ.VManageUI.20.12.1-_17.12.1_N.14	Try to Select Range of Site ID's under Administartion Resource Groups.	Failed	CSCwf51256
ENJ.VManageUI.20.12.1-_17.12.1_N.15	Try to Create a Workflow under Quick Connect.	Failed	CSCwf51333
ENJ.VManageUI.20.12.1-_17.12.1_N.16	Verify the logs in Device 360 page under System Status > Crash.	Failed	CSCwf54260
ENJ.VManageUI.20.12.1-_17.12.1_N.17	Verify the logs in Device 360 page under System Status > Reboot.	Failed	CSCwf54278
ENJ.VManageUI.20.12.1-_17.12.1_N.18	Try to Enable the options under Table settings of the Configurations > Devices.	Passed	CSCwf58010
ENJ.VManageUI.20.12.1-_17.12.1_N.19	Try to Install Certificate under configuration > Certificates and verify it.	Passed	CSCwf58039
ENJ.VManageUI.20.12.1-_17.12.1_N.20	Navigate to Administartion > Manage Users and try to edit the user group.	Passed	CSCwf63112
ENJ.VManageUI.20.12.1-_17.12.1_N.21	Create a new user access in Manager User with Network Hierarchy and verify it.	Passed	CSCwf67622

SD-AVC

Logical ID	Title	Status	Defect ID
ENJ.SDAVC.20.12.1-_17.12.1_N.01	Try to Get the Token key After Umbrella registration in Vmanage	Failed	CSCwh03750
ENJ.SDAVC.20.12.1-_17.12.1_N.02	Check the Scroll bar up and down button is not funtioning properly in Device_Export page-Chrome Browser	Failed	CSCwf71058
ENJ.SDAVC.20.12.1-_17.12.1_N.03	Check the Scroll bar up and down button is not funtioning properly in Security - Advanced Malware Protection - Chrome Browser	Failed	CSCwf71095
ENJ.SDAVC.20.12.1-_17.12.1_N.04	Check the Zscalar registration was Enabled by Wrong User ID ,User name or not	Failed	CSCwf85947
ENJ.SDAVC.20.12.1-_17.12.1_N.05	Check Status of the SD-AVC Cloud connector When disabled or Enabled in Vmanage	Failed	CSCwf63724
ENJ.SDAVC.20.12.1-_17.12.1_N.06	Check the Zscalar registration was Enabled by Wrong Partner base URl or not	Failed	CSCwh03140
ENJ.SDAVC.20.12.1-_17.12.1_N.07	Check the Status of the PMT credentials When disabled or Enabled in Vmanage	Failed	CSCwf77155
ENJ.SDAVC.20.12.1-_17.12.1_N.08	Check the Status of the PSmart Account credentials When disabled or Enabled in Vmanage	Failed	CSCwf77138

SDRA

Logical ID	Title	Status	Defect ID
ENJ.SDRA.20.12.1_17.12.1_N01	Create Enterprise root CA for the SDRA Configuration Group	Passed	
ENJ.SDRA.20.12.1_17.12.1_N02	Enable SDRA and associate the device with default values	Passed	
ENJ.SDRA.20.12.1_17.12.1_N03	Install the CA certificate in client machine to get the Authorized & connected.	Passed	
ENJ.SDRA.20.12.1_17.12.1_N04	Verify authentication with ISE server	Passed	
ENJ.SDRA.20.12.1_17.12.1_N05	Verify IP Pool for IPV4 is mandatory parameter and ipv6 pool is not mandatory	Passed	
ENJ.SDRA.20.12.1_17.12.1_N06	Verify IP Pool & Change the size of the pool	Passed	
ENJ.SDRA.20.12.1_17.12.1_N07	Verify Virtual-Access template is up & provide ip address to client machine	Passed	
ENJ.SDRA.20.12.1_17.12.1_N08	Verify pool deletion should not be allowed once it being hold by device.	Passed	
ENJ.SDRA.20.12.1_17.12.1_N09	Verify authentication with CA server	Passed	
ENJ.SDRA.20.12.1_17.12.1_N10	Create AAA policy and attach the profile with Attributes in ISE for AAA	Passed	
ENJ.SDRA.20.12.1_17.12.1_N11	Enable SDRA, and Associate with device with user defined values--> Radius/eap with user authentication	Passed	

ENJ.SDRA.20.12.1_17.12.1_N12	Add the network device with service vpn and provide preshared key in ISE for AAA	Passed	
ENJ.SDRA.20.12.1_17.12.1_N13	Verify Delete of SDRA configuration when configuration group is already deployed	Passed	
ENJ.SDRA.20.12.1_17.12.1_N14	Verify copy of SDRA configuration when configuration group is already deployed	Passed	
ENJ.SDRA.20.12.1_17.12.1_N15	Verify IKEv2 setting SA Lifetime	Passed	

QoS

Logical ID	Title	Status	Defect ID
ENJ.QoS.20.12.1_17.12.1_N01	To monitor the data traffic using dscp value in QOS marking class map policy.	Passed	
ENJ.QoS.20.12.1_17.12.1_N02	To configure the LLQ with a priority percent for a single traffic	Passed	
ENJ.QoS.20.12.1_17.12.1_N03	To configure the LLq and CBWFQ with a multiple traffic of class map policy.	Passed	
ENJ.QoS.20.12.1_17.12.1_N04	To configure a single rate two color policing with cir 128kbpa for a single traffic	Passed	
ENJ.QoS.20.12.1_17.12.1_N05	To configure the two-rate policing with Cir 500kbps and peak rate of 1mbps.	Passed	
ENJ.QoS.20.12.1_17.12.1_N06	To configure a shaping on the bandwidth percent queues in a qos traffic	Passed	
ENJ.QoS.20.12.1_17.12.1_N07	To configure an average shaping range with 8000kbps	Passed	
ENJ.QoS.20.12.1_17.12.1_N08	To configure an adaptive shaping of upstream bandwidth range with 6000kbps	Passed	
ENJ.QoS.20.12.1_17.12.1_N09	To configure a bandwidth allocation based on data traffic in a queue	Passed	
ENJ.QoS.20.12.1_17.12.1_N10	To configure the queue limit allocation based on the traffic in queue (using WRED).	Passed	
ENJ.QoS.20.12.1_17.12.1_N11	To configure the Per-VPN QOS and generate the traffic and check the performance.	Passed	

ENJ.QoS.20.12.1_17.12.1_N12	To configure a knob of vm traffic forwarding class queue using cli.	Passed	
ENJ.QoS.20.12.1_17.12.1_N13	To delete the knob of vm traffic class of queue user choice and check the global attribute id using cli.	Passed	
ENJ.QoS.20.12.1_17.12.1_N14	To configure an adaptive shaping of downstream bandwidth range with 8000kbps.	Passed	
ENJ.QoS.20.12.1_17.12.1_N15	To configure the forwarding qos and generate the traffic using v-manage feature template.	Passed	
ENJ.QoS.20.12.1_17.12.1_N16	To remove the knob of vm traffic class of queue user choice and check the running policy in the device.	Passed	
ENJ.QoS.20.12.1_17.12.1_N17	To check that knob is applied under the policy in app and flow visibility while attaching the template.	Passed	
ENJ.QoS.20.12.1_17.12.1_N18	To generate the 5000 bulk vmanage traffic to the cEdge device and check the forwarding queue packet transmitted.	Passed	
ENJ.QoS.20.12.1_17.12.1_N19	To generate the bulk of data and check the default queue after removing a new knob queue then check in vmanage.	Passed	
ENJ.QoS.20.12.1_17.12.1_N20	To disable and enable the new knob of vm forwarding class of queue and check the client global policy.	Passed	
ENJ.QoS.20.12.1_17.12.1_N21	To monitor the drop of packets in queue 0 before and after configuring the new knob vm fwd. queue.	Passed	

ENJ.QoS.20.12.1_17.12.1_N22	To configure the vmanage traffic forwarding of queue and check the statistics in the cli.	Passed	
ENJ.QoS.20.12.1_17.12.1_N23	To check the default queue of packet increases or decreases with and without generating the bulk traffic and conf that new knob.	Passed	
ENJ.QoS.20.12.1_17.12.1_N24	To configure the vmanage forward classing in queue 7 with user choice and check the performance.	Passed	
ENJ.QoS.20.12.1_17.12.1_N25	To configure the vmanage traffic forwarding queue and check the option enabled it or not.	Passed	

Adhoc

Logical ID	Title	Description	Status	Defect ID
ENJ.Adhoc_20.12.1_17.12.1_N.01	Try to Upgrade the C8200/C8300 Devices to 17.12 EFT-1 and reload it.	Upgrade the edge routers with 17.12 Eft-1 and reload the device and observe the behaviour.	Passed	CSCwf62681
ENJ.Adhoc_20.12.1_17.12.1_N.02	Try to Add a Service VPN Template for feature template and observe the behaviour	Try to add a Service VPN Template under Feature template and observe the behaviour of it.	Passed	CSCwf73767
ENJ.Adhoc_20.12.1_17.12.1_N.03	Check the page get malfuntioned for the below 6 events security, firewall, malware, url filtering, top threats and intrustion prevention	Check all the 6 events click on view details and try to move to other options in main menu. The options view details is not closing and move to other page	Passed	CSCwf71122
ENJ.Adhoc_20.12.1_17.12.1_N.04	Check the Scroll bar up and down button is not funtioning properly in Device_Export page- Chrome Browser_firefox	Check the Scroll bar is malfunctioning & now able to scroll up and down frequently and no up and down arrows in the right side of the page in chrome browser and firefox	Failed	CSCwf71165
ENJ.Adhoc_20.12.1_17.12.1_N.05	Check the Scroll bar up and down button is not funtioning properly in Configuration -> Certificate Authority- Chrome Browser_firefox	Check the Scroll bar up and down button is not funtioning properly in Configuration -> Certificate Authority- Chrome Browser_firefox	Failed	CSCwf71176

ENJ.Adhoc_20.12.1_17.12.1_N.06	Check the page get malfuntioned for the Software Repository page	Check the Software Repository and Click on view details and try to move to other options in main menu. The options view details is not closing and move to other page	Failed	CSCwf72625
ENJ.Adhoc_20.12.1_17.12.1_N.07	Check the page get malfuntioned for the Software Repository - Firmware page	Check the page get malfuntioned for the Software Repository - Firmware page	Failed	CSCwf72638
ENJ.Adhoc_20.12.1_17.12.1_N.08	Check the page get malfuntioned for the Administration -> License Management	Check the page get malfuntioned for the Administration -> License Management	Failed	CSCwf72695

Related Documents

- Related Documentation, on page 80

Related Documentation

Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release 17.12 Release Notes

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/17-12/sd-wan-rel-notes-xe-17-12.html

Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.12

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

Cisco SD-WAN Router Configuration Guide, Cisco IOS XE Release 17.12

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/routing/ios-xe-17/routing-book-xe/transport-gw.html

Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.12

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/centralized-policy.html#concept_a2t_gjw_5xb

Cisco SD-WAN Monitor and Maintain Configuration Guide,Cisco IOS XE Release 17.12

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/m-alarms-events-logs.html#c_Alarms_12333.xml

Cisco SD-WAN Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.12

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/cloudonramp/ios-xe-17/cloud-onramp-book-xe/cloud-onramp-multi-cloud-aws.html

Cisco SD-WAN Security Configuration Guide, Cisco IOS XE Release 17.12

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/intrusion-prevention.html