Test Results Summary for IOS XE SD-WAN for Japan (Release Version 20.11.1/17.11.1)

First Published: 2023-05-07

Last Modified: 2023-05-15

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 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 20.11.1 - IOS XE 17.11.1
- 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

Acronyms

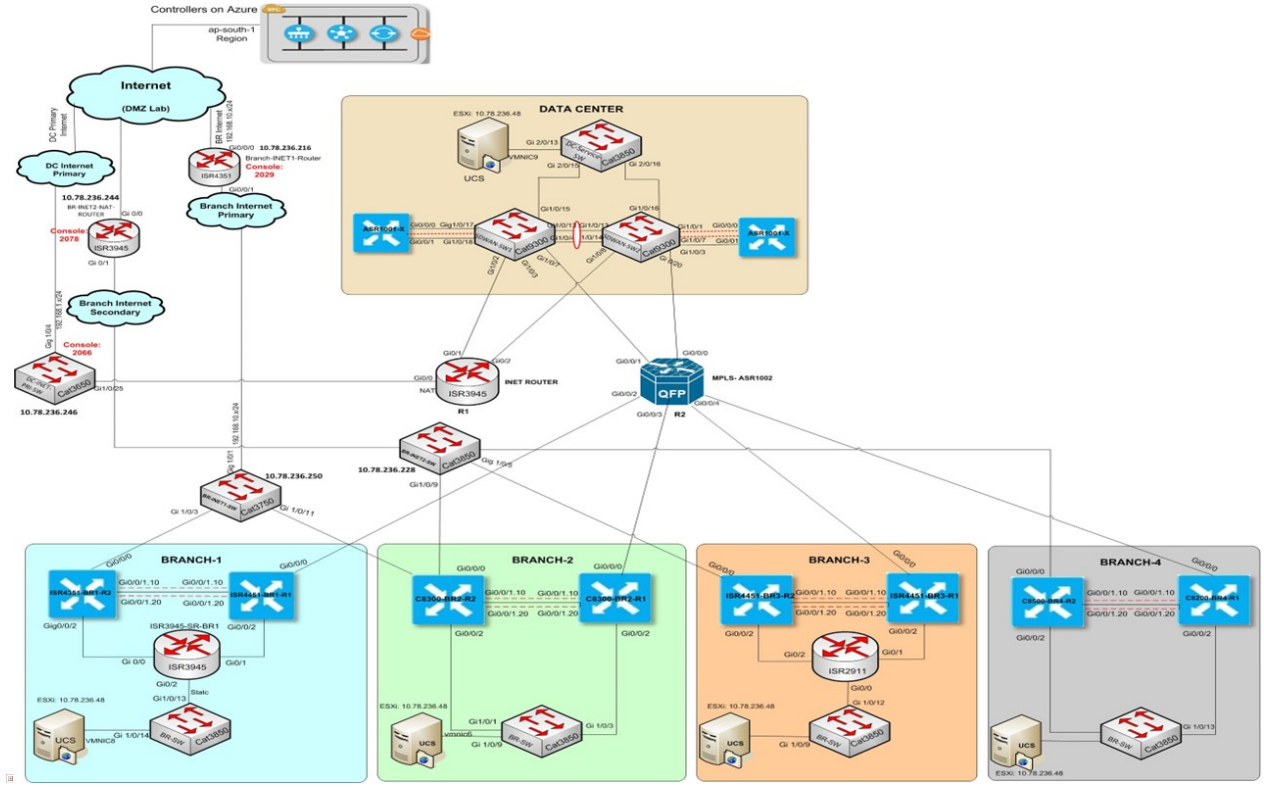
Acronym	Description
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AF	Address-family
API	Application Programming Interface
ASN	Autonomous System Number
ASR	Aggregation Services Routers
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BR	Branch
BR Site	Branch 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



Component Matrix

Applications	Category	Component	Version
Controller Network	Virtual Network	vBond	20.11.1
		vManage	20.11.1
		vSmart	20.11.1
	Switch	Cat 9K PoE	17.2
Communications Infrastructure	IOS XE SDWAN	C8300, C8200 & C8500L	17.11.1
		ISR4461	17.11.1
UCS	UCSC-C240-M5SX	ESXi Host	6.0, 6.5
Client	Operating System	End point	Windows 10
	Browsers	Mozilla	110.0
		Chrome	110.0.5481.100

What's New ?

SDWAN 20.11.1 - IOS XE 17.11.1 Solution testing

- Configuration Groups and Feature Profiles (Phase III)
- Grouping of Alarms,Grouping of Events
- Cisco SD-WAN Remote Access Configuration
- TLOC Extension Over IPv6
- IPv6 DIA and Static Route Tracker
- Log Action for both Localized and Centralized Data Policies
- Co-Management Improved Granular Configuration for Resource group features
- Route Aggregation on Border Routers and Transport Gateways
- Download Output of OMP Routes
- Quarantine support for Revoked devices
- GRE-in-UDP
- Ability to put router generated traffic into the queue of user choice [CLI template]
- Support for MSDP to Interconnect Cisco SD-WAN and Non-SD-WAN Domains
- Port Forwarding with NAT DIA Using a Loopback Interface
- Destination NAT Support in case of NAT DIA –SDWAN CLI
- NAT ALG Support - Phase II
- SDWAN CLI c8000V SDWAN Enterprise Certificate Support

Open Caveats

CDETS ID	Title
CSCwe69154	Tunnel status remains unchange, shows up/up when shutting down the physical sub-Interface - IPv6
CSCwf08671	Ipsec/ikev2 -Not able to connect AnyConnect client, authentic and authorization failure with the SDRA
CSCwf11016	ux2.0 Config group-Ipv4 address filed is accepting the numbers in any number format other than ipadd
CSCwe63882	Identity Service Engine - Not able to drag/scroll the scroll bar - Chrome browser
CSCwf00050	Cannot Change App Route Visuaization Fields if generation unsuccessful
CSCwf08143	SCM Wizard TAC Case Scroll Bar is not Working as Expected.
CSCwe80782	Troubleshooting Option is not working in Device Monitoring Dashboard.
CSCwf01714	Rogue Tag Assignation based on Tagging history for devices
CSCwf01763	Duplicated shared configuration Groups for profiles
CSCwe88079	With incorrect crlserver vmanage getting error request timedout instead of failed to update
CSCwf09461	ACL Sequence name column is Saving with empty character
CSCwf08360	While configuring Cisco security keyID name is created with empty space, Can't Able to Set CustomTime
CSCwf09775	Eye Button is not working for show the credentials in PMT credentials on 20.11
CSCwf09720	Wrong Client ID & Client Secret is accepted when PMT is Enabled
CSCwf09126	In Sig credentials When go to View option,view button Is available but close button is not available
CSCwf08136	Accepting wrong Org-id ,wrong Api-key, wrong api-secret for Sig Credential Settings
CSCwf08075	Eye Button is not working for show the password in Smart account credentials on 20.11
CSCwe84126	The tracker Status is showing UP, Without the endpoint is not Reachable

CSCwe49766	1st Export file download skipped when 2nd download started
CSCwe49713	Pagination CSV export file missing headers
CSCwf01664	Misleading Operational Command Admin-tech Download
CSCwf01562	MRF Aggregate failing OMP process
CSCwf01687	Monitoring App Route Visualization is redirecting to Unknown/Irrelevant page
CSCwf08046	Wrong Credentials Smart Account is getting Enabled 20.11.1a its validation issue
CSCwe82284	Enterprise CA is Successfully Authorized in Administration setting But its not Display Authorized

Resolved Caveats

CDETS ID	Title
CSCwe45262	Add pool option is not available under global option
CSCwe50829	Real time monitoring: changes made in columns preferences isn't reflecting in the output.
CSCwf00174	Failed to Display the Add Feature Profile in Configuration Group
CSCwe46674	Unable to view the Events/Events Page by using device action tab
CSCwe68430	RBAC Application Monitoring permission missing/mapped wrongly
CSCwf10876	Command argument order reversed for MRF aggregate region with aggregate-only

New Features

Configuration Groups and Feature Profiles

Logical ID	Title	Description	Status	Defect ID
ENJ.UX 2.0 Config20.11.1_17.11.1_N01	To create an ipv4 global sdra pool in network hierarchy	In network hierarchy page, for creating a sdra pool by using ipv4 type .	Passed	
ENJ.UX 2.0 Config20.11.1_17.11.1_N02	To create an ipv6 global SDRA pool in network hierarchy	In network hierarchy page, for creating a sdra pool by using ipv46 type .	Passed	
ENJ.UX 2.0 Config20.11.1_17.11.1_N03	To edit ipv4 global sdra pool in network hierarchy	To check able to edit the existing ipv4 global sdra pool details in network hierarchy	Passed	
ENJ.UX 2.0 Config20.11.1_17.11.1_N04	To delete ipv4 global sdra pool in network hierarchy	To perform the delection of existing ipv4 global sdra pool which is not in use in network hierarchy	Passed	
ENJ.UX 2.0 Config20.11.1_17.11.1_N05	To edit ipv6 global sdra pool in network hierarchy	To check able to edit the existing ipv6 global sdra pool details in network hierarchy	Passed	
ENJ.UX 2.0 Config20.11.1_17.11.1_N06	To delete ipv6 global sdra pool in network hierarchy	To perform the delection of the existing ipv6 global sdra pool which is not in use in network hierarchy	Passed	
ENJ.UX 2.0 Config20.11.1_17.11.1_N07	To edit global system Ip pool in network hierarchy	To check able to edit the existing pool type as system ip details in network hierarchy	Passed	
ENJ.UX 2.0 Config20.11.1_17.11.1_N08	To delete global system Ip pool in network hierarchy	To delete the existing pool type created system ip in network hierarchy	Passed	

ENJ.UX 2.0 Config.20.11.1_17.11.1_N09	To check whether able to display ipv4/v6 global sdra pool utilization	To view the utlilization of pool in network hierarchy page in the pool table under used it should display ipv4/v6 global sdra pool utilization	Passed	
ENJ.UX 2.0 Config.20.11.1_17.11.1_N10	To display the ip address per site in network hierarchy	In network hierarchy page, checking the ip address per site	Passed	
ENJ.UX 2.0 Config.20.11.1_17.11.1_N11	To create read permissions for System parcel	Creating a System parcel with read permission and check the permissions.	Passed	
ENJ.UX 2.0 Config.20.11.1_17.11.1_N12	To create read permissions for Service parcel	Creating a Service parcel with read permission and check the permissions.	Passed	
ENJ.UX 2.0 Config.20.11.1_17.11.1_N13	To add node - site, area, pool under global option	Adding the site, area, pool by using node under global option	Passed	CSCwe45262
ENJ.UX 2.0 Config.20.11.1_17.11.1_N14	To check the Ip's are allocated/use based on subnet/ip address	Checking the Ip's that are allocated in the pool use based on subnet/ip address assigned.	Passed	
ENJ.UX 2.0 Config.20.11.1_17.11.1_N15	To create write permissions for Teleworker parcel	Creating a Teleworker parcel with write permission and check the permissions.	Passed	
ENJ.UX 2.0 Config.20.11.1_17.11.1_N16	To create write permissions for Service parcel	Creating a Service parcel with write permission and check the permissions.	Passed	

ENJ.UX 2.0 Config20.11.1_17.11.1_N17	To create write permissions for system parcel	Creating a System parcel with write permission and check the permissions.	Passed	
ENJ.UX 2.0 Config20.11.1_17.11.1_N18	To create write permissions for Transport parcel	Creating a Transport parcel with write permission and check the permissions.	Passed	
ENJ.UX 2.0 Config20.11.1_17.11.1_N19	To edit node and pool under global option	To perform the edit option on node and pool under global option	Passed	
ENJ.UX 2.0 Config20.11.1_17.11.1_N20	To Create an ipv4 pool under global option	Creating a pool by using ipv4 type under global option In network hierarchy page.	Passed	
ENJ.UX 2.0 Config20.11.1_17.11.1_N21	To Create an ipv6 pool under global option	Creating a pool by using ipv6 type under global option In network hierarchy page.	Passed	
ENJ.UX 2.0 Config20.11.1_17.11.1_N22	To check the device variable for Thousand eye parcel has read / write permissions on Cat 8k platform	For Thousand eye parcel with read / write permissions on Cat 8k platform ,check the read/write permissions for device variables are working	Passed	
ENJ.UX 2.0 Config20.11.1_17.11.1_N23	To check the device variable for Thousand Eyes parcel has read / write permissions on ISR platform	For Thousand eye parcel with read / write permissions on ISR platform ,check the read/write permissions for device variables are working	Passed	

ENJ.UX 2.0 Config.20.11.1_17.11.1_N24	To deploy the configuration group and check the device variable are editable for admin users	Checking the device variable are editable for admin users while deploying the configuration group.	Passed	
ENJ.UX 2.0 Config.20.11.1_17.11.1_N25	To provide read permission for AAA parcel and check device variable are editable for generic users while deploying the device	Creating AAA parcel with read permissions and checking the device variables are editable for generic users while deploying the device	Passed	
ENJ.UX 2.0 Config.20.11.1_17.11.1_N26	To provide write permission for service parcel and check device variable are editable for generic users while deploying the device	Creating service parcel with write permission and check device variable are editable for generic users while deploying the device	Failed	CSCwf01763
ENJ.UX 2.0 Config.20.11.1_17.11.1_N27	To create device variable for basic parcel and check the device variable are editable while deploying the device	Creating a basic parcel and check the device variable are editable while deploying the device	Passed	
ENJ.UX 2.0 Config.20.11.1_17.11.1_N28	To create a same device variable description for different parcels	To check the read/write permissions by creating a same device variables for different parcels.	Passed	
ENJ.UX 2.0 Config.20.11.1_17.11.1_N29	To check default system device variables have read/write permissions under basic parcel	To check default system device variables have read/write permissions under basic parcel	Passed	
ENJ.UX 2.0 Config.20.11.1_17.11.1_N30	Use export option to check edit the writeable device variables	Device variables with write permissions use export option and perform the edit.	Passed	

ENJ.UX 2.0 Config.20.11.1_17.11.1_N31	To create IP pool using system ip under network hierarchy	By using network hierarchy option,Creating a IP pool with system ip .	Passed	
ENJ.UX 2.0 Config.20.11.1_17.11.1_N32	To create IP pool using system ip under global	By using global option,Creating a IP pool with system ip	Passed	
ENJ.UX 2.0 Config.20.11.1_17.11.1_N33	To create a cisco security feature under system profile using configuration group.	By using cisco security it will work under the system profile and using configuration group	Failed	CSCwf08360
ENJ.UX 2.0 Config.20.11.1_17.11.1_N34	To create and delete tracker feature under service profile using configuration group.	Using the delete tracker feature using service profile under configuration group	Failed	CSCwf09461
ENJ.UX 2.0 Config.20.11.1_17.11.1_N35	To create a Tracker Group feature under Transport profile using configuration group	By using Group feature under Transport profile using configuration group	Passed	

Grouping of Alarms-Grouping of Events

Logical ID	Title	Description	Status	Defect ID
ENUX20_2011.1_17.11.1_N01	To download alarms and events using export option to check the attribute fields.	By using export option download the alarms and events to check the attribute fields.	Passed	
ENUX20_2011.1_17.11.1_N02	To view the critical alarms of site 1 and major alarms of site 2 by using multiple site filter	By using multiple site filter select the site 1 as critical alarm and site 2 with major and apply the filter	Passed	
ENUX20_2011.1_17.11.1_N03	To filter/group by the alarms based on TYPE	Based on filter as TYPE,filter the alarms	Passed	
ENUX20_2011.1_17.11.1_N04	To filter/group by the alarms based on Object(site)	Based on filter as OBJECT with type as site ,filter the alarms	Passed	
ENUX20_2011.1_17.11.1_N05	To filter/group by the alarms based on Object (Device)	Based on filter as OBJECT with type as Device ,filter the alarms	Failed	CSCwe80782
ENUX20_2011.1_17.11.1_N06	To filter/group the alarms based on Severity (Critical, Major, Medium)	To perform the filtering of alarms based on Severity with Critical, Major and Medium)	Passed	
ENUX20_2011.1_17.11.1_N07	To filter/group the alarms based on Severity (Minor and Info)	To perform the filtering of alarms based on Severity as Minor .	Passed	
ENUX20_2011.1_17.11.1_N08	To check the alarms based on logs on chart format	To view the alarms on chart format by using navigation through logs	Passed	
ENUX20_2011.1_17.11.1_N09	To filter the alarms using advanced filter options	Applying the filter for the alarms by using advanced filter options	Passed	

ENUX20_2011.1_17.11.1_N10	To view the device alarms using site topology	By using the site topology,check whether able to view the device alarms	Passed	
ENUX20_2011.1_17.11.1_N11	To check Top alarms using Top alarms dash let	To view the Top alarms using Top alarms dashlet fir single site using overview.	Passed	
ENUX20_2011.1_17.11.1_N12	To check alarms and events using site topology	By using site topology navigate to alarms and events pages and check the alarms and events.	Passed	
ENUX20_2011.1_17.11.1_N13	To check alarms and events under device action tab	By using the device action tab for a selected device , check the alarms and events .	Failed	CSCwe46674
ENUX20_2011.1_17.11.1_N14	To create a maximum of 6 filters and check the alarms notification using AND operation	Checking the alarms notification using AND operation by Creating a maximum of 6 filters	Passed	
ENUX20_2011.1_17.11.1_N15	To create a maximum of 6 filters and check the alarms notification using OR operation	Checking the alarms notification using OR operation by Creating a maximum of 6 filters	Passed	
ENUX20_2011.1_17.11.1_N16	To filter the events using advanced filter option based on the type using OR operation	By using advanced filter option filter the events using OR operation	Passed	
ENUX20_2011.1_17.11.1_N17	To clear the input values using clear button after applying the filtered values	After applying the filter option,check whether able to clear the input vales	Passed	
ENUX20_2011.1_17.11.1_N18	To check whether alarms are displayed using related events sidebar	By using related events sidebar , check whether able to view the alarms .	Passed	

ENUX20_2011.1_17.11.1_N19	To customize the alarm notification page using add/edit list page under alarm notification view	In alarm notification,check able to add/edit the alarm notifications.	Passed	
ENUX20_2011.1_17.11.1_N20	To customize the alarm notification page using delete list page under alarm notification view	In alarm notification,check able to delete the alarm notifications.	Passed	
ENUX20_2011.1_17.11.1_N21	To filter the events using advanced filter option based on the type using AND operation	By using advanced filter option filter the events using AND operation	Passed	
ENUX20_2011.1_17.11.1_N22	To filter the Events by Object (Device)	Based on filter as OBJECT with type as Device ,filter the events.	Passed	
ENUX20_2011.1_17.11.1_N23	To filter the events by Object (Site)	Based on filter as OBJECT with type as site ,filter the events	Passed	
ENUX20_2011.1_17.11.1_N24	Acknowledge the alerts and check whether it has displayed under notification side bar	Acknowledge the alerts and check whether it has displayed under notification side bar	Passed	
ENUX20_2011.1_17.11.1_N25	To filter events by using Events severity	Performing the filtering on events by applying the Events severity	Passed	

Cisco SD-WAN Remote Access Configuration

Logical ID	Title	Description	Status	Defect ID
ENJ.SDRA_20.11.1_17.11.1_N01	Create Enterprise root CA for the SDRA Configuration Group	To Verify Enterprise root CA	Failed	CSCwf11016
ENJ.SDRA_20.11.1_17.11.1_N02	Edit Enterprise CA in the Config group	To chek the edit option for the enterprise root ca	Passed	
ENJ.SDRA_20.11.1_17.11.1_N03	Enable SDRA and associate the device with default values	To check the sdra option is enable and able to associate the device	Passed	
ENJ.SDRA_20.11.1_17.11.1_N04	Verify AAA Pre-shared	To Check the AAA option with default values	Passed	
ENJ.SDRA_20.11.1_17.11.1_N05	Install the CA certificate in client machine to get the Authorized & connected.	Install and Verify the CA certificate in client machine	Failed	CSCwf08671
ENJ.SDRA_20.11.1_17.11.1_N06	SDRA with ipsec using ipv4	To verify the ipsec using ipv4 address	Passed	
ENJ.SDRA_20.11.1_17.11.1_N07	Verify authentication with ISE server	To Verify Authentication using ISE server for Radius	Passed	
ENJ.SDRA_20.11.1_17.11.1_N08	Verify authentication with CA server	To Verify Authentication using CA server for Certificate	Passed	
ENJ.SDRA_20.11.1_17.11.1_N09	Create AAA policy and attach the profile with Attributes in ISE for AAA	Enable ISE server policy and profile with Attributes	Passed	
ENJ.SDRA_20.11.1_17.11.1_N010	Disable SDRA	To verify Disable option in SDRA	Passed	

ENJSDRA_20.11.1_17.11.1_N011	Verify Edit of SDRA configuration EDIT when configuration group is already deployed.	To verify edit option in sdra	Passed	
ENJSDRA_20.11.1_17.11.1_N012	Enable SDRA, and Associate with device with user defined values--> Radius/eap with user authentication	Check the Radius/eap with user authentication	Passed	
ENJSDRA_20.11.1_17.11.1_N013	Enable SDRA, and Associate with device with user defined values--> Radius/eap with user and device authentication+ anyconnect profile download	Check the Radius/eap with user and device authentication+ anyconnect profile download	Passed	
ENJSDRA_20.11.1_17.11.1_N014	Verify Authentication Tab with AnyConnect Radius/EAP	To check the Authenticaton tab with defined values with ISE	Passed	
ENJSDRA_20.11.1_17.11.1_N015	Verify AAA Policy configuration with option "Specify name" with password other than default	To check the AAA config with password	Passed	
ENJSDRA_20.11.1_17.11.1_N016	Verify AAA Policy configuration with option "Specify name" with default values	To check the AAA config with default values	Passed	
ENJSDRA_20.11.1_17.11.1_N017	Verify IP Pool for IPV4 is mandatory parameter and ipv6 pool is not mandatory	To check the ip pool for the ipv4 and ipv6 not required	Passed	

ENJSDRA_20.11.1_17.11.1_N018	Check RA VPN user can able to auth successfully and connect the edge RA router	To check ra vpn user can able to auth ISE and edge router	Passed	
ENJSDRA_20.11.1_17.11.1_N019	Check RA VPN user in Windows machine can able to successfully access the web server	To check ra vpn user can able to connect windows machine with any connect client	Passed	
ENJSDRA_20.11.1_17.11.1_N020	Verify GRE and try to establish the RAVPN	To enable gre in the tunnel interface and verify the connection	Passed	
ENJSDRA_20.11.1_17.11.1_N021	Add the network device with service vpn and provide preshared key in ISE for AAA	In ISE server add the network device and provide preshare key	Passed	
ENJSDRA_20.11.1_17.11.1_N022	Verify Delete of SDRA configuration when configuration group is already deployed	To Vefiy delete option in the sdra config group	Passed	
ENJSDRA_20.11.1_17.11.1_N023	Verify copy of SDRA configuration when configuration group is already deployed	To Vefiy Edit option in the sdra config group	Passed	
ENJSDRA_20.11.1_17.11.1_N024	Verify IP Pool for IPV4	To check the ip pool for the ipv4	Passed	
ENJSDRA_20.11.1_17.11.1_N025	Verify IKEv2 setting SA Lifetime	To check the SA lifetime	Passed	
ENJSDRA_20.11.1_17.11.1_N026	Check IKEv2 SA parameters for the session, the username, and the assigned IP.	To check the SA parameters	Passed	

ENJSDRA_20.11.1_17.11.1_N027	Verify Authentication Tab -> Radius Group Name	To verify radius group name	Passed	
ENJSDRA_20.11.1_17.11.1_N028	Verify IP Pool & Change the size of the pool	To check the ip pool can be changed with different subnet mask	Passed	
ENJSDRA_20.11.1_17.11.1_N029	Verify Virtual-Access template is up & provide ip address to client machine	To check the virtual -access template created while establishing the session	Passed	
ENJSDRA_20.11.1_17.11.1_N030	Verify pool deletion should not be allowed once it being hold by device.	To verify the created pool is able to delete	Passed	
ENJSDRA_20.11.1_17.11.1_N031	Switch to another SDRA profile to multiple config group and verify	To verify the sdra connection with Mulitple profiles configured	Passed	
ENJSDRA_20.11.1_17.11.1_N032	Edit ISE radius settings in vManage and verify session.	To verify the edit setting in vManage for ISE	Passed	

TLOC Extension Over IPv6

Logical ID	Title	Description	Status	Defect ID
ENJJIPV6_TE20.11.1_17.11.1_N01	Enable ipv6 tloc extn for the Physical interface	To enable the ipv6 tloc using physical interface	Failed	CSCwe69154
ENJJIPV6_TE20.11.1_17.11.1_N02	Disable ipv6 tloc extn for the Physical interface	To disable the ipv6 tloc using physical interface	Passed	
ENJJIPV6_TE20.11.1_17.11.1_N03	Config ipv6 tloc ext for the physical interface using vManage CLI template	To enable the ipv6 tloc for physical interface using vManage cli Template	Passed	
ENJJIPV6_TE20.11.1_17.11.1_N04	Enable ipv6 tloc extn for the sub interface	To enable the ipv6 tloc using sub interface	Passed	
ENJJIPV6_TE20.11.1_17.11.1_N05	Disable ipv6 tloc extn for the sub interface	To disable the ipv6 tloc using sub interface	Passed	
ENJJIPV6_TE20.11.1_17.11.1_N06	Config ipv6 tloc ext for the physical sub interface using vManage CLI template	To enable the ipv6 tloc for sub interface using vManage cli Template	Passed	
ENJJIPV6_TE20.11.1_17.11.1_N07	Enable ipv6 tloc extn for the loopback interface for extended wan circuits	To enable the ipv6 tloc using loopback interface	Passed	
ENJJIPV6_TE20.11.1_17.11.1_N08	Disable ipv6 tloc extn for the loopback interface for extended wan circuits	To disable the ipv6 tloc using loopback interface	Passed	
ENJJIPV6_TE20.11.1_17.11.1_N09	Config ipv6 tloc ext for the Loopback interface using vManage CLI template	To enable the ipv6 tloc for loopback interface using vManage cli Template	Passed	

ENJIPV6_TE.20.11.1_17.11.1_N010	Verify NAT66 for the physical interface	Enable NAT66 for the physical interface for ipv6 address	Passed	
ENJIPV6_TE.20.11.1_17.11.1_N011	Verify NAT66 for the physical sub interface	Enable NAT66 for the sub interface for ipv6 address	Passed	
ENJIPV6_TE.20.11.1_17.11.1_N012	Verify NAT66 for the Loopback Interface	Enable NAT66 for the loopback interface for ipv6 address	Passed	
ENJIPV6_TE.20.11.1_17.11.1_N013	Verify IPV6 NAT DIA with NAT66	Enable DIA for the interface & verify with NAT66	Passed	
ENJIPV6_TE.20.11.1_17.11.1_N014	Verify Implicit IPv6 ACL on TLOC tunnel interface	Configure Implicit ACL for ipv6 and verify the logs	Passed	
ENJIPV6_TE.20.11.1_17.11.1_N015	Verify IPv6 TLOC is dual stack capable – when both v4 and v6 are present, tunnel is built on top of either v4 or v6 and not both, based on the preference configured	Verify the Dual stack is working with tloc extn	Passed	
ENJIPV6_TE.20.11.1_17.11.1_N016	Check that dual sub interface is having ipv6 tloc extn traffic	To check the tloc extn for the dual sub interface	Passed	
ENJIPV6_TE.20.11.1_17.11.1_N017	Check that dual sub interface is having ipv6 tloc extn traffic using vManage CLI template	To check the tloc extn for the dual sub interface using vManage CLI template	Passed	
ENJIPV6_TE.20.11.1_17.11.1_N018	Verify IPV6 tloc extn with ACL to permit the traffic	Configure ACL to permit the traffic	Passed	
ENJIPV6_TE.20.11.1_17.11.1_N019	Check ipv6 tloc extn is advertise in OMP routes	Check ipv6 tloc extn omp routes are getting advertised	Passed	

ENJJIPV6_TE20.11.1_17.11.1_N020	Verify ipv6 tloc end to end reachibility using l2 & l3 interface & check for BFD session	Check the end to end reacablity with ipv6 tloc extn and verify	Passed	
ENJJIPV6_TE20.11.1_17.11.1_N021	Verify ipv4 and ipv6 tloc using port preservation	Verify ipv4 and ipv6 tloc using port preservation	Passed	

Log Action for both Localized and Centralized Data Policies

Logical ID	Title	Description	Status	Defect ID
ENJLADP20.11.1_17.11.1_N01	Configure centralize policy and add log-action check the first packet within 5 minute active-flow syslog	When Configure centralize policy and add log-action check the first packet within 5 minute active-flow syslog .	Passed	
ENJLADP20.11.1_17.11.1_N02	Configure localized policy and add log-action check the first packet within 5-minute active-flow syslog	Through Configure localized policy and add log-action check the first packet within 5-minute active-flow syslog	Passed	
ENJLADP20.11.1_17.11.1_N03	Check the log format it should correct Syslog format is similar to v-Edge or not	When Configure centralize policy check the log formet	Passed	
ENJLADP20.11.1_17.11.1_N04	Check the c-Edge has log policer when enabled by default with 25 log/sec threshold	When enabled the log policer Check the default log	Passed	
ENJLADP20.11.1_17.11.1_N05	Check also logs locally to a SQL DB, which V-manage pulls periodically and display in monitor login screen	When policy is enabled Check also logs locally to a SQL DB, which V-manage pulls periodically and display in monitor login screen	Passed	
ENJLADP20.11.1_17.11.1_N06	Configure sdwan uses Polaris High Speed Logging infra to perform “implicit-acl-logging"	When Configure sdwan uses Polaris check the High Speed Logging infra to perform “implicit-acl-logging"	Passed	
ENJLADP20.11.1_17.11.1_N07	When HSL is registered check to send IPFIX records to internal IP	After HSL is registered check to send IPFIX records to internal IP or not	Passed	

ENJLADP20.11.1_17.11.1_N08	When HSL is also setup with templates then check for the IPFIX records	Verify when HSL is also setup with templates then check for the IPFIX records or not	Passed	
ENJLADP20.11.1_17.11.1_N09	When FTM process binds to this IP and Port then check receives the data records	Verify when FTM process binds to this IP and Port then check receives the data records	Passed	
ENJLADP20.11.1_17.11.1_N10	Check in the log life-cycle a Packet hits an implicit ACL or not	Check in the log life-cycle a Packet hits an implicit ACL or not and capture the log	Passed	
ENJLADP20.11.1_17.11.1_N11	Configer centralize policy check in the log life-cycle If "implicit_acl_logging" is enabled, an IPFIX record is constructed with fields from packet header and record is sent to HSL or not	Configer centralize policy check in the log life-cycle If "implicit_acl_logging" is enabled, an IPFIX record is constructed with fields from packet header and record is sent to HSL or not and verify the log	Passed	
ENJLADP20.11.1_17.11.1_N12	Check in the log life-cycle if HSL module sends the record to IP:Port setup or not	Verify the log life-cycle if HSL module sends the record to IP:Port setup or not	Passed	
ENJLADP20.11.1_17.11.1_N13	Check in the log life-cycle if FTM receives this IPFIX record, decodes it, forms a string and does syslog or not	Verify the log life-cycle if FTM receives this IPFIX record, decodes it, forms a string and does syslog or not	Passed	
ENJLADP20.11.1_17.11.1_N14	Check in the log life-cycle Ex log is seen or not	Check in the log life-cycle Ex log is seen or not and verify the log	Passed	

ENJLADP20.11.1_17.11.1_N15	Check in the log life-cycle If an external syslog server is configured, log will be sent over to it by Polaris Infra or not	Verify the log life-cycle If an external syslog server is configured, log will be sent over to it by Polaris Infra or not	Passed	
ENJLADP20.11.1_17.11.1_N16	Check the Current implicit ACL configuration in V-manage	Verify the Current implicit ACL configuration in V-manage and capture the logs	Passed	
ENJLADP20.11.1_17.11.1_N17	Configure Data Policy with match app-list app, action log,For matching IPv4 traffic check the log is generated or not	Configure Data Policy with match app-list app, action log,For matching IPv4 traffic check the log is generated or not with verify the logs	Passed	
ENJLADP20.11.1_17.11.1_N18	Configure AAR Policy with match app-list app, action log. For matching IPv4 traffic, check the log is generated or not	Configure AAR Policy with match app-list app, action log. For matching IPv4 traffic, check the log is generated or not and Verify	Passed	
ENJLADP20.11.1_17.11.1_N19	Configure ACL Policy with match destination-ip, action log. For matching IPv4 traffic,check the log is generated or not.	Configure ACL Policy with match destination-ip, action log. For matching IPv4 traffic,check the log is generated or not and verify	Passed	
ENJLADP20.11.1_17.11.1_N20	Configure AAR Policy with match app-list app, action log. For matching IPv4 traffic, check the log is generated or not	Configure AAR Policy with match app-list app, action log. For matching IPv4 traffic, check the log is generated or not and Verify	Passed	
ENJLADP20.11.1_17.11.1_N21	Configure AAR and DP policy for IPv6 supported or not	Configure AAR and DP policy for IPv6 supported or not and Verify	Passed	

ENJLADP20.11.1_17.11.1_N22	Check the Log-rate-limit can be left at default value for syslog	Check the Log-rate-limit can be left at default value for syslog and capture the log	Passed	
ENJLADP20.11.1_17.11.1_N23	Check the QOS or Route Policy able to configure or not.	Check the QOS or Route Policy able to configure or not and verify	Passed	
ENJLADP20.11.1_17.11.1_N24	Check the localized policy knob to throttle number of logs per second at the source (Data Path) itself with CPU performence	Check the localized policy knob to throttle number of logs per second at the source (Data Path) itself with CPU performance and verify	Passed	
ENJLADP20.11.1_17.11.1_N25	Check the Log-rate-limit can be left at default value for syslog	Check the Log-rate-limit can be left at default value for syslog and capture the log	Passed	
ENJLADP20.11.1_17.11.1_N26	Connect IPerf with the device and send the stream and add the log policy check the log by throughput Testing	Connect IPerf with the device and send the stream and add the log policy check the log by throughput Testing and verify	Passed	

Co-Management Improved Granular Configuration for Resource group feature

Logical ID	Title	Description	Status	Defect ID
ENJRBAC20.11.1_17.11.1_N.01	Configure RBAC Resource Group access	Grant User Group Resource Group, log in as the user and verify access	Passed	
ENJRBAC20.11.1_17.11.1_N.02	Monitor All Pill access	Grant User Group access to All Pills, log in as the user and verify they're accessible	Passed	
ENJRBAC20.11.1_17.11.1_N.03	Monitor Few Pill access	Grant User Group access to Few Pills, log in as the user and verify they're accessible	Passed	CSCwe68430
ENJRBAC20.11.1_17.11.1_N.04	Configure RBAC Report access	Grant User Group access to Report, log in as the user and verify access	Passed	
ENJRBAC20.11.1_17.11.1_N.05	Configure RBAC Certificate Read access.	Grant User Group Read access to Certificates, log in as the user and verify access	Passed	
ENJRBAC20.11.1_17.11.1_N.06	Configure RBAC Certificate Write access.	Grant User Group Write access to Certificates, log in as the user and verify access	Passed	
ENJRBAC20.11.1_17.11.1_N.07	Observe Reboot Read access.	Grant User Group Read access to Reboot, log in as the user and verify access	Passed	
ENJRBAC20.11.1_17.11.1_N.08	Configure RBAC Reboot Write access.	Grant User Group Write access to Reboot, log in as the user and verify access	Passed	

ENJ.RBAC.20.11.1_17.11.1_N.09	Configure RBAC Application routing access	Grant User Group access to Application routing, log in as the user and verify access	Passed	
ENJ.RBAC.20.11.1_17.11.1_N.10	Configure RBAC Service VPN access	Grant User Group access to Service VPN, log in as the user and verify access	Passed	
ENJ.RBAC.20.11.1_17.11.1_N.11	Execute GET API Read Permission for System Profile	Grant User Group Read access to System Profile, verify successful GET	Passed	
ENJ.RBAC.20.11.1_17.11.1_N.12	Execute PUT API Read Permission for System Profile	Grant User Group Read access to System Profile, verify unsuccessful PUT	Passed	
ENJ.RBAC.20.11.1_17.11.1_N.13	Execute PUT API Write Permission for System Profile	Grant User Group Write access to System Profile, verify successful PUT	Passed	
ENJ.RBAC.20.11.1_17.11.1_N.14	Execute GET API Read Permission for Other Profile	Grant User Group Read access to Other Profile, verify successful GET	Passed	
ENJ.RBAC.20.11.1_17.11.1_N.15	Execute PUT API Read Permission for Other Profile	Grant User Group Read access to Other Profile, verify unsuccessful PUT	Passed	
ENJ.RBAC.20.11.1_17.11.1_N.16	Execute PUT API Write Permission for Other Profile	Grant User Group Write access to Other Profile, verify successful PUT	Passed	
ENJ.RBAC.20.11.1_17.11.1_N.17	Execute GET API Read Permission for Transport Profile	Grant User Group Read access to Transport Profile, verify successful GET	Passed	

ENJRBAC20.11.1_17.11.1_N.18	Execute PUT API Read Permission for Transport Profile	Grant User Group Read access to Transport Profile, verify unsuccessful PUT	Passed	
ENJRBAC20.11.1_17.11.1_N.19	Execute PUT API Write Permission for Transport Profile	Grant User Group Write access to Transport Profile, verify successful PUT	Passed	
ENJRBAC20.11.1_17.11.1_N.20	Execute GET API Read Permission for Service Profile	Grant User Group Read access to Service Profile, verify successful GET	Passed	
ENJRBAC20.11.1_17.11.1_N.21	Execute PUT API Read Permission for Service Profile	Grant User Group Read access to Service Profile, verify unsuccessful PUT	Passed	
ENJRBAC20.11.1_17.11.1_N.22	Execute PUT API Write Permission for Service Profile	Grant User Group Write access to Service Profile, verify successful PUT	Passed	
ENJRBAC20.11.1_17.11.1_N.23	GET API Reflects GPS Parcel Creation Under Transport Profile	Create GPS Parcel Under Transport Profile, and see it's reflected GET API output	Passed	

Route Aggregation on Border Routers and Transport Gateways

Logical ID	Title	Description	Status	Defect ID
ENJ.HSDWAN.20.11.1_17.11.1_N.01	Route Aggregation from Service to Both core and access with shut no shut	Configure Route Aggregation from Service to Both core and access, then verify with shut no shut	Failed	CSCwf01562
ENJ.HSDWAN.20.11.1_17.11.1_N.02	Route Aggregation from Service to Access-only with shut no shut	Configure Route Aggregation from Service to Access-only, then verify with shut not shut	Passed	
ENJ.HSDWAN.20.11.1_17.11.1_N.03	Route Aggregation from Service to Access-only without region	Configure Route Aggregation from Service to Access-only without region	Passed	
ENJ.HSDWAN.20.11.1_17.11.1_N.04	Route Aggregation from Service to Both core and access without region	Configure Route Aggregation from Service to Both core and access without region	Passed	
ENJ.HSDWAN.20.11.1_17.11.1_N.05	Route Aggregation from Service to Access-only removing and adding region	Configure Route Aggregation from Service to Access-only removing and adding region	Passed	
ENJ.HSDWAN.20.11.1_17.11.1_N.06	Route Aggregation from Service to Both core and access removing and adding region	Configure Route Aggregation from Service to Both core and access, and verify removing and adding region	Passed	
ENJ.HSDWAN.20.11.1_17.11.1_N.07	Route Aggregation on Transport Gateway	Configure and verify Route Aggregation on a Transport Gateway device	Passed	

ENJHSDWAN20.11.1_17.11.1_N.08	Optimized OMP TLOC and path advertisement	Configure OMP TLOC and path advertisement and verify OMP TLOCs	Passed	
ENJHSDWAN20.11.1_17.11.1_N.09	Optimized OMP TLOC and path advertisement with Incompatible colors	Configure OMP TLOC and path advertisement with Incompatible colors and verify Incompatible colors are omitted	Passed	
ENJHSDWAN20.11.1_17.11.1_N.10	Route Aggregation from Service to Access-only	Configure Route Aggregation from Service to Access-only	Passed	
ENJHSDWAN20.11.1_17.11.1_N.11	Route Aggregation from Service to Both core and access	Configure Route Aggregation from Service to Both core and access	Passed	CSCwf10876
ENJHSDWAN20.11.1_17.11.1_N.12	Configure Control policy route affinity	Configure Control policy for route affinity and verify affinity	Passed	
ENJHSDWAN20.11.1_17.11.1_N.13	Configure Control policy TLOC affinity	Configure Control policy for TLOC affinity and verify affinity	Passed	

Download Output of OMP Routes

Logical ID	Title	Descrption	Status	Defect ID
ENJ.Pagination.20.11.1_17.11.1_N.01	OMP IPv4 Advertised Routes in CSV Format	From Real Time page choose OMP IPv4 Advertised Routes and download them in CSV Format	Failed	CSCwe49713
ENJ.Pagination.20.11.1_17.11.1_N.02	OMP IPv4 Advertised Routes in JSON Format	From Real Time page choose OMP IPv4 Advertised Routes and download them in JSON Format	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.03	Cancelling OMP IPv4 Advertised Routes in CSV Format	From Real Time page choose OMP IPv4 Advertised Routes and download them in CSV Format and cancel download	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.04	Cancelling OMP IPv4 Advertised Routes in JSON Format	From Real Time page choose OMP IPv4 Advertised Routes and download them in JSON Format and cancel download	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.05	OMP IPv4 Received Routes in CSV Format	From Real Time page choose OMP IPv4 Received Routes and download them in CSV Format	Failed	CSCwe50829
ENJ.Pagination.20.11.1_17.11.1_N.06	OMP IPv4 Received Routes in JSON Format	From Real Time page choose OMP IPv4 Received Routes and download them in JSON Format	Passed	

ENJ.Pagination.20.11.1_17.11.1_N.07	Cancelling OMP IPv4 Received Routes in CSV Format	From Real Time page choose OMP IPv4 Received Routes and download them in CSV Format and cancel download	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.08	Cancelling OMP IPv4 Received Routes in JSON Format	From Real Time page choose OMP IPv4 Received Routes and download them in JSON Format and cancel download	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.09	OMP IPv4 Advertised Routes in CSV Formatafter removing routes	Before and after removing Advertised routes, from Real Time page choose OMP IPv4 Advertised Routes and download them in CSV Format	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.10	OMP IPv4 Advertised Routes in JSON Format after removing routes	Before and after removing Advertised routes, from Real Time page choose OMP IPv4 Advertised Routes and download them in JSON Format	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.11	Cancelling OMP IPv4 Advertised Routes in CSV Format after removing routes	Before and after removing Advertised routes, from Real Time page choose OMP IPv4 Advertised Routes and download them in CSV Format and cancel download	Passed	

ENJ.Pagination.20.11.1_17.11.1_N.12	Cancelling OMP IPv4 Advertised Routes in JSON Format after removing routes	Before and after removing Advertised routes, from Real Time page choose OMP IPv4 Advertised Routes and download them in JSON Format and cancel download	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.13	OMP IPv4 Received Routes in CSV Format after removing routes	From Real Time page download OMP IPv4 Received Routes in CSV Format after removing routes	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.14	OMP IPv4 Received Routes in JSON Format after removing routes	From Real Time page download OMP IPv4 Received Routes in JSON Format after removing routes	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.15	Cancelling OMP IPv4 Received Routes in CSV Format after removing routes	From Real Time page download OMP IPv4 Received Routes in CSV Format after removing routes and cancel download	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.16	Cancelling OMP IPv4 Received Routes in JSON Format after removing routes	From Real Time page download OMP IPv4 Received Routes in JSON Format after removing routes and cancel download	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.17	Create same data CSV File while File Generation is in progress	From Real Time page start CSV File download while previous same CSV File Generation is in progress	Passed	

ENJ.Pagination.20.11.1_17.11.1_N.18	Create same data JSON File while File Generation is in progress	From Real Time page start JSON File download while previous different File while File Generation is in progress	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.19	Create different data CSV File while File Generation is in progress	From Real Time page start CSV File download while previous different File while File Generation is in progress	Failed	CSCwe49766
ENJ.Pagination.20.11.1_17.11.1_N.20	Create different data JSON File while File Generation is in progress	From Real Time page create different data JSON File while File Generation is in progress	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.21	Create same data CSV File right after cancelling File Generation	From Real Time page create same data CSV File right after cancelling previous File Generation	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.22	Create same data JSON File right after cancelling File Generation	From Real Time page create same data JSON File right after cancelling previous File Generation	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.23	Create same data CSV File some time after cancelling File Generation	From Real Time page create same data CSV File some time after cancelling previous File Generation	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.24	Create same data JSON File some time after cancelling File Generation	From Real Time page create same data JSON File some time after cancelling previous File Generation	Passed	

ENJ.Pagination.20.11.1_17.11.1_N.25	Create different data CSV File right after cancelling File Generation	From Real Time page create different data CSV File right after cancelling previous File Generation	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.26	Create different data JSON File right after cancelling File Generation	From Real Time page create different data JSON File right after cancelling previous File Generation	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.27	Create same data JSON File right after cancelling CSV File Generation	From Real Time page create same data JSON File right after cancelling previous CSV File Generation	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.28	Create same data CSV File right after cancelling JSON File Generation	From Real Time page create same data CSV File right after cancelling previous JSON File Generation	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.29	Create different data JSON File right after cancelling CSV File Generation	From Real Time page create different data JSON File right after cancelling previous CSV File Generation	Passed	
ENJ.Pagination.20.11.1_17.11.1_N.30	Create different data CSV File right after cancelling JSON File Generation	Create different data CSV File right after cancelling previous JSON File Generation	Passed	

Quarantine support for Revoked devices

Logical ID	Title	Description	Status	Defect ID
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N01	To enable CRL Quarantine setting on UI for certificate revocation (CRL) via vpn 0.	To perform the certification based quarantine on certificate revocation list using vpn 0	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N02	To enable CRLQuarantine setting on UI for certificate revocation(CRL) via vpn 512.	To perform the certification based quarantine on certificate revocation list using vpn 512	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N03	To verify alarms on vManage when CRL is enabled using CRL quarantine option.	When CRL is enabled using CRL quarantine option check whether able to get the alarms on vManage	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N04	To verify alarms on vManage when CRL is disabled.	When CRL is disbled ,check whether able to get the alarms on vManage	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N05	To verify alarms and certificate revocation on vManage when controllers (vManage,Smart controller) is revoked.	To perform certificate revocation on vManage check whether able to get the alarms for certificate revocation on controllers.	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N06	To verify device certificate is revoked on vManage.	Perform the certificate revocation on device and check the whether able to get the alarrm on vManage.	Passed	

ENJ.UX 2.0_CRL_20.11.1_17.11.1_N07	To enable CRL revocation with incorrect URL via VPN 0 and check CRL behavior.	Check the CRL revocation option on vmanage with incorrect URL via VPN 0 and check the CRL behavior.	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N08	To enable CRL revocation option on vManage UI with incorrect URL via VPN 512 and check CRL behavior.	Check the CRL revocation with incorrect URL via VPN 512 and check the CRL behavior.	Failed	CSCwe88079
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N09	To change the interval for CRL using quarantine option and check whether vManage has pull CRL	Perform the certificate based quarantine using certificate revocation list by changing the interval time.	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N10	To enable CRL quarantine setting option on vManage with incorrect URL via VPN 512 and check CRL behaviour.	Check the CRL quarantine option with incorrect URL via VPN 512 and check the CRL behavior.	Failed	CSCwe88079
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N11	To enable CRL revocation option on vManage for certification revocation via VPN 0	Perform the certificate revocation on certificate revocation list via VPN 0	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N12	To enable CRL revocation option on vMange for certificate revocation via VPN 512	Perform the certificate revocation on certificate revocation list via VPN 512	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N13	To enable CRL quarantine setting option on vManage with incorrect URL via VPN 0 and check CRL behaviour.	Check the CRL quarantine option with incorrect URL via VPN 0 and check the CRL behavior.	Passed	

ENJ.UX 2.0_CRL_20.11.1_17.11.1_N14	To verify the different states of certificate revocation during CRL quarantine process	To verify the different states of certificate revocation during CRL quarantine process	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N15	. To check the alarms when CA CRL server is not reachable.	When CA CRL server is not reachable check whether able to get the alarm for it.	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N16	To enable CRL Quarantine setting on UI for certification revocation (CRL) on cat8kv platform.	Cat8kv platform perform CRL Quarantine setting on UI for certification revocation (CRL) .	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N17	To enable certificate revocation on UI for certification revocation (CRL) on cat8kv platform.	Perform the certificate revocation on UI for certification revocation (CRL) on cat8kv platform.	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N18	To check the generated syslogs when crl quarantine is enabled	When crl quarantine is enabled, check whether able to generate the syslogs	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N19	To check the generated syslogs when crl quarantine is disabled.	When crl quarantine is disabled, check whether able to generate the syslogs	Passed	
ENJ.UX 2.0_CRL_20.11.1_17.11.1_N20	To check the generated syslogs when certificate revocation on controllers	When performing the certificate revocation on controllers, check whether able to get the generated syslogs	Passed	

ENJ.UX 2.0_CRL_20.11.1_17.11.1_N21	To check the generated syslogs when edge device been quarantined	When performing the certificate based quarantine on device, check whether able to get the generated syslogs	Passed	

GRE-in-UDP

Logical ID	Title	Description	Status	Defect ID
ENGRE_20.11.1_17.11.1_N01	Verify can able to do GRE in UDP using IPV6	To check the GRE in UDP tunnel using IPV6	Passed	
ENGRE_20.11.1_17.11.1_N02	Verify can able to do GRE in UDP using IPV4	To check the GRE in UDP tunnel using IPV4	Passed	
ENGRE_20.11.1_17.11.1_N03	Verify can able to do GRE in UDP using IPV6 using private ckt	To check the GRE in UDP tunnel using IPV6 via private ckt	Passed	
ENGRE_20.11.1_17.11.1_N04	Verify can able to do GRE in UDP using Preference	To check the GRE in UDP tunnel using Preference	Passed	
ENGRE_20.11.1_17.11.1_N05	Verify can able to do GRE in UDP using IPV4 using private ckt	To check the GRE in UDP tunnel using IPV4 via private ckt	Passed	
ENGRE_20.11.1_17.11.1_N06	Verify can able to do GRE in UDP using IPV4 using Public ckt	To check the GRE in UDP tunnel using IPV4 via public ckt	Passed	
ENGRE_20.11.1_17.11.1_N07	Disable the gre-in udp in sdwan tunnel	To disbale or Shut the gre tunnels	Passed	
ENGRE_20.11.1_17.11.1_N08	Enable gre-in udp on both the end and verify the truth table	To check the GRE in UDP tunnel in both end using truth table	Passed	
ENGRE_20.11.1_17.11.1_N09	Enable gre-in udp in local and remote as gre and verify the truth table	To check the GRE in local and GRE in UDP as remote tunnel using truth table	Passed	
ENGRE_20.11.1_17.11.1_N10	Enable gre in local and remote as gre-in udp and verify the truth table	To check the GRE in local and GRE as remote tunnel using truth table	Passed	

ENGRE_20.11.1_17.11.1_N11	Enable gre in local and remote as gre and verify the truth table	To check the GRE in UDP as local and GRE as remote tunnel using truth table	Passed	
ENGRE_20.11.1_17.11.1_N12	verify we can able to access GRE-in UDP in vManage CLI template using ipv4	To check the GRE in UDP using vManage CLI Template	Passed	
ENGRE_20.11.1_17.11.1_N13	verify we can able to access GRE-in UDP using Weight	To check the GRE in UDP tunnel using weight	Passed	
ENGRE_20.11.1_17.11.1_N14	Verify the GRE in udp can be configured per tloc	To check the GRE in UDP for tloc interface	Passed	
ENGRE_20.11.1_17.11.1_N15	Enable gre-in udp on both the end with Keepalive interval	To enable keepalive interval for the GRE in UDP tunnel	Passed	
ENGRE_20.11.1_17.11.1_N16	Enable gre-in udp on both the end with ipv6 and ACL	To enable ACL for the GRE in UDP tunnel using ipv6 address	Passed	

IPv6 DIA and Static Route Tracker

Logical ID	Title	Description	Status	Defect ID
ENJIPV6_DIA_20.11.1_17.11.1_N01	DIA trackers status with tracker threshold configured with its maximum/minimum range value for ipv6	To check and track the DIA tracker for threshold max/min range values using ipv6	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N02	IPv6 Dual Endpoint Support For Interface Status tracking with on cisco IOS XE SD-Wan Device.	To track the ipv6 dual endpoint using interface tracking	Failed	CSCwe84126
ENJIPV6_DIA_20.11.1_17.11.1_N03	IPv6 Dual Endpoint tracker in tracking group with Boolean OR operation on cisco IOS XE SD-Wan Device	To track the ipv6 dual endpoint using tracking group by boolean OR operation	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N04	DIA IPv6 Dual endpoint Tracking for interface in tracking Group by VManage	To track the ipv6 dual endpoint using interface tracking using vManage	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N05	DIA tracking with IPv6 Dual Endpoint in Tracker group By using Boolean AND operation	To track the ipv6 dual endpoint using tracking group by boolean AND operation	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N06	Instead of DIA tracker Configure the NAT Fallback tracker for CEdge Router	To check the NAT fallback tracket instead DIA tracker	Passed	

ENJIPV6_DIA_20.11.1_17.11.1_N07	DIA Dual endpoint tracker combination of DNS and DNS with AND operation by CLI	By using Command line interface we have configure the tracker combination of DNS and DNS with AND operation.	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N08	DIA IPv6 Dual endpoint tracker combination of IP and IP with OR operation by CLI	By using Command line interface we have configure the tracker combination of IP and IP with OR operation.	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N09	IPv6 DIA Tracker for Track the endpoint With Internet transport link.	To track the ipv6 dual endpoint using interface trasport link	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N10	DIA IPv6 Dual endpoint tracker combination of DNS and IP with OR operation By CLI	By using Command line interface we have configure the tracker combination of DNS and IP with OR operation.	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N11	Apply tracker to IPv6 Dialer Interface using Encapsulation with PPP	By using VManage we have configure the Dailer Interface using Encapsulation with PPP	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N12	Apply tracker to IPv6 Dailer Interface using Encapsulation with HDLC	By using VManage we have configure the Dailer Interface using Encapsulation with HDLC	Passed	

ENJIPV6_DIA_20.11.1_17.11.1_N13	Dailer interface for IPv6 DIA by CHAP in PPP Encapsulation	Configure by using VManage in PPP Authentication with CHAP	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N14	DIA Tracker with IPv6 Dailer interface by using PPP Authentication with PAP	Configure by using VManage in PPP Authentication with PAP	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N15	Define a new IPv6 HTTPS tracker using an IPv6 endpoint API-URL	Configure new IPv6 HTTPS tracker using an IPv6 endpoint API-URL	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N16	Apply defined IPv6 tracker to a supported IPv6 interface	Configure defined IPv6 tracker to a supported IPv6 interface	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N17	IPv4 DIA Tracker for IPv6 Tunnel	Configure IPv4 DIA Tracker for IPv6 Tunnel	Passed	
ENJIPV6_DIA_20.11.1_17.11.1_N18	DIA trackers status with tracker threshold configured with its Out of range value for ipv6	To check the DIA trackers status with tracker threshold configured with its Out of range value for ipv6	Passed	

Ability to put router generated traffic into the queue of user choice

Logical ID+A308:E328	Title	Description	Status	Defect ID
ENJ.QOS.20.11.1_17.11.1_N.01	To configure a knob of vm traffic forwarding class queue using cli.	To Generate and configure the knob of vm traffic forwarding class queue using cli.	Passed	
ENJ.QOS.20.11.1_17.11.1_N.02	To configure a knob of vm traffic forwarding class queue using vmanage cli template	Monitor and configure knob of vm traffic forwarding class queue using vmanage cli template	Passed	
ENJ.QOS.20.11.1_17.11.1_N.03	To delete the knob of vm traffic class of queue user choice and check the global attribute id using cli.	Remove the knob of vm traffic class of queue user choice and check the global attribute id using cli.	Passed	
ENJ.QOS.20.11.1_17.11.1_N.04	To remove the knob of vm traffic class of queue user choice and check the running policy in the device	Delete the knob of vm traffic class of queue user choice and check the running policy in the device	Passed	
ENJ.QOS.20.11.1_17.11.1_N.05	To configure a knob of vm traffic forwarding class queue then generate the traffic and check the performance in cli.	Generate and configure a knob of vm traffic forwarding class queue the traffic and check the performance in cli.	Passed	
ENJ.QOS.20.11.1_17.11.1_N.06	To create a multiple queue with vm traffic forwarding class and check the fwd. queue after generating the traffic.	Configure multiple queue with vm traffic forwarding class and check the fwd. queue after generating the traffic.	Passed	

ENJ.QOS.20.11.1_17.11.1_N.07	To configure a knob of vm traffic forwarding class queue then generate the traffic and check the performance in vmanage	To Generate and monitor after configuring a knob of vm traffic forwarding class queue then generate the traffic and check the performance in vmanage	Passed	
ENJ.QOS.20.11.1_17.11.1_N.08	To generate the 5000 bulk vmanage traffic to the cEdge device and check the forwarding queue packet transmitted	Generate the 5000 bulk vmanage traffic to the cEdge device and check the forwarding queue packet transmitted	Passed	
ENJ.QOS.20.11.1_17.11.1_N.09	To configure the vmanage traffic forwarding queue and check the option enabled it or not.	Monitor the vmanage traffic forwarding queue and check the option enabled it or not.	Passed	
ENJ.QOS.20.11.1_17.11.1_N.10	To generate the bulk of data in the default queue and check the packet after removing the fwd. queue in cli.	To Monitor and generate the bulk of data in the default queue and check the packet after removing the fwd. queue in cli.	Passed	
ENJ.QOS.20.11.1_17.11.1_N.11	To configure the vmanage fwd classing in queue 7 with user choice and check the performance.	Configuring the vmanage fwd classing in queue 7 with user choice and check the performance.	Passed	
ENJ.QOS.20.11.1_17.11.1_N.12	To generate the bulk of data and check the default queue after removing a new knob queue in vmanage	Monitor and generate the bulk of data and check the default queue after removing a new knob queue in vmanage	Passed	
ENJ.QOS.20.11.1_17.11.1_N.13	To reload the cEdge device and check the fwd queue policy still performing or not.	Check the fwd queue policy still performing or not after reload the cEdge device	Passed	

ENJ.QOS.20.11.1_17.11.1_N.14	To check the running policy after shut the wan interface while having a Tloc transport connections.	Create and check the running policy after shut the wan interface while having a Tloc transport connections.	Passed	
ENJ.QOS.20.11.1_17.11.1_N.15	To monitor the drop of packets in queue 0 before and after configuring the new knob vm fwd queue.	Configure and monitor the drop of packets in queue 0 before and after configuring the new knob vm fwd queue.	Passed	
ENJ.QOS.20.11.1_17.11.1_N.16	To apply the new knob in the TLOC Interface and the check the forward queueing user choice.	Configure and apply the new knob in the TLOC Interface and the check the forward queueing user choice.	Passed	
ENJ.QOS.20.11.1_17.11.1_N.17	To configure the vmanage traffic fwd of queue and check the statistics in the cli.	Generate by configuring the vmanage traffic fwd of queue and check the statistics in the cli.	Passed	
ENJ.QOS.20.11.1_17.11.1_N.18	To disable and enable the new knob of vm fwd class of queue and check the client global policy.	Check the client global policy by disable and enable the new knob of vm fwd class of queue	Passed	
ENJ.QOS.20.11.1_17.11.1_N.20	To check the default queue of packet inc or dec with without generating the bulk traffic and also conf that new knob.	Moitor and check the default queue of packet inc or dec with without generating the bulk traffic and also conf that new knob.	Passed	
ENJ.QOS.20.11.1_17.11.1_N.21	To check that knob is applied under the policy in app and flow visibility while attaching the template.	Configure the policy and check that knob is applied under the policy in app and flow visibility while attaching the template.	Passed	

Support for MSDP to Interconnect Cisco SD-WAN and Non-SD-WAN Domains

Logical ID	Title	Descrption	Status	Defect ID
ENJ.MSDP20.11.1_17.11.1_N01	Enable MSDP in cedge devices	Enable MSDP in cedge devices	Passed	
ENJ.MSDP20.11.1_17.11.1_N02	Disable MSDP in cedge devices	Disable MSDP in cedge devices	Passed	
ENJ.MSDP20.11.1_17.11.1_N03	Configure MSDP between cedge and service router in dual homed setup	Configure MSDP between cedge and service router in dual homed setup	Passed	
ENJ.MSDP20.11.1_17.11.1_N04	Configure MSDP between cedge and service router in single homed setup	Configure MSDP between cedge and service router in single homed setup	Passed	
ENJ.MSDP20.11.1_17.11.1_N05	Check MSDP SA between cedge and service router in DC end	Check MSDP SA between cedge and service router in DC end	Passed	
ENJ.MSDP20.11.1_17.11.1_N06	Check MSDP SA between cedge and souce as DC end	Check MSDP SA between cedge and souce as DC end	Passed	
ENJ.MSDP20.11.1_17.11.1_N07	Check MSDP SA between cedge and cedge in DC end	Check MSDP SA between cedge and cedge in DC end	Passed	
ENJ.MSDP20.11.1_17.11.1_N08	Check MSDP SA between cedge and non sdwan	Check MSDP SA between cedge and non sdwan	Passed	
ENJ.MSDP20.11.1_17.11.1_N09	Check OMP SA between cedge and cedge in different site	Check OMP SA between cedge and cedge in different site	Passed	
ENJ.MSDP20.11.1_17.11.1_N010	Check OMP SA between different site from source to receiver end	Check OMP SA between different site from source to receiver end	Passed	
ENJ.MSDP20.11.1_17.11.1_N011	Validate the translation of OMP SA to MSDP SA using S,G State	Validate the translation of OMP SA to MSDP SA using S,G State	Passed	

ENJ.MSDP20.11.1_17.11.1_N012	Validate the translation of OMP SA to MSDP SA using S,G state	Validate the translation of OMP SA to MSDP SA using S,G state	Passed	
ENJ.MSDP20.11.1_17.11.1_N013	configure MSDP using vManage CLI template	configure MSDP using vManage CLI template	Passed	
ENJ.MSDP20.11.1_17.11.1_N014	Configure MDP usng Add-on CLI template	Configure MDP usng Add-on CLI template	Passed	
ENJ.MSDP20.11.1_17.11.1_N015	Configure MSDP using ux2.0 Configuration group	Configure MSDP using ux2.0 Configuration group	Passed	

Port Forwarding with NAT DIA Using a Loopback Interface

Logical ID	Title	Description	Status	Defect ID
ENJ.LPF.20.11.1_17.11.1_N.01	Configure the loopback interface is support for nat DIA port forwording	By using loopback interface is support for DIA port forwording	Passed	
ENJ.LPF.20.11.1_17.11.1_N.02	Configure the loopack suport for port forwording in UDP port	By using loopback interface is support for port forwording with UDP Port	Passed	
ENJ.LPF.20.11.1_17.11.1_N.03	Configure Inbound Port Forwarding for loopback and verify	By using loopback interface Configure Inbound Port Forwarding and verify	Passed	
ENJ.LPF.20.11.1_17.11.1_N.04	Configure Out-bound Port Forwarding for loopback and verify	By using loopback interface Configure Out-bound Port Forwarding and verify	Passed	
ENJ.LPF.20.11.1_17.11.1_N.05	Configure tunnel with Port Forwarding for loopback and verify Tunnel health	By using loopback interface is support for port forwording	Passed	
ENJ.LPF.20.11.1_17.11.1_N.06	Verify the Overlay-Interface-Transport when loopback tunnel should be up	By using loopback tunnel should be up with overlay interface	Passed	
ENJ.LPF.20.11.1_17.11.1_N.07	Configure and verify cEdge NAT-DIA port forwarding Loopback support	By using loopback interface is support for DIA port forwording	Passed	
ENJ.LPF.20.11.1_17.11.1_N.08	Configure and verify cEdge NAT ALG support for DIA flows	By using cEdge NAT ALG support for DIA flows with port forwarding	Passed	
ENJ.LPF.20.11.1_17.11.1_N.09	Configure cEdge NAT GateKeeper for enhancements and verify..	By using cEdge NAT GateKeeper for enhancements and verify.	Passed	

ENJLPF20.11.1_17.11.1_N.10	Use SAP static address mapping in interface sub-net range extensively and check SAP Statics	By using SAP static address mapping in interface sub-net range extensively and check SAP Statics	Passed	
ENJLPF20.11.1_17.11.1_N.11	Configure the source static TCP port with loopback interface with egress WAN interface	By using source static TCP port with loopback interface with egress WAN interface	Passed	
ENJLPF20.11.1_17.11.1_N.12	Check Traffic flows with TLOC as a DIA interface and verify	By using Traffic flows with TLOC as a DIA interface and verify	Passed	
ENJLPF20.11.1_17.11.1_N.13	Check TCP traffic from DIA with server in service side vpn 0	By using TCP traffic from DIA with server in service side vpn 0	Passed	
ENJLPF20.11.1_17.11.1_N.14	Configure multiple servers for same public loopback address in the servers side	By using multiple servers for same public loopback address in the servers side	Passed	
ENJLPF20.11.1_17.11.1_N.15	Check when Send traffic for multiple servers from DIA port its receving or not.	By using the send traffic for multiple servers from DIA port its receving or not	Passed	
ENJLPF20.11.1_17.11.1_N.16	Check the cEdge NAT single tenancy limit supported or not	By using cEdge NAT single tenancy limit supported or not	Passed	
ENJLPF20.11.1_17.11.1_N.17	To check the timing session for NAT port translations	By using timing session to check the NAT port translations	Passed	
ENJLPF20.11.1_17.11.1_N.18	Configure DIA port forwarding with interface address and port with port change with vrf	By using DIA port forwarding with interface address and port with port change with vrf.	Passed	

ENJLPF20.11.1_17.11.1_N.19	To configure the static NAT Port forwarding in UDP port 5001 using cli template.	By using static NAT Port forwarding in UDP port 5001 using cli template.	Passed	
ENJLPF20.11.1_17.11.1_N.20	Configure cEdge NAT with Destination NAT for DIA and verify.	By using cEdge NAT with Destination NAT for DIA and verify.	Passed	

Destination NAT Support in case of NAT DIA

Logical ID	Title	Description	Status	Defect ID
ENJ.Des_Nat.20.11.1_17.11.1_N.001	To configure NAT DIA in wan Interface	Applying NAT configuration to wan interface and check Nat translations	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.002	To configure data policy with destination DIA and Nat fallback	Configure data policy by enabiling nat fall back and apply destination NAT in policy	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.003	configure data policy with NAT DIA counter	Confiure data policy with Nat counter and push policy to edge device	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.004	To configure Destination Nat with DIA interface overload	Confiure Destination NAT to wan interface and overload the NAT configured interface check NAT behaviour	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.005	To configure endpoint tracker for ip in wan interface with DIA interface overload	Configure endpoint tracker for ip in wan interface with DIA interface overload and check the translations	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.006	To configure to shut DIA path using tracker and verify the Nat translations	Configure to shutdown DIA path using tracker that applied to NAT configured interface and verify the Nat translations	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.007	To configure Loopback overload with Destination Nat	Configure the Loopback interface and apply NAT config in Loopback interface and check DEST NAT	Passed	

ENJ.Des_Nat.20.11.1_17.11.1_N.008	To Configure applying Destination Nat in loopback overload with fallback	Configure applying Destination Nat in loopback overload with fallback and checking the NAT Behaviour	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.009	configure to apply the tracker shut to loopback overload and validate the traffic	Configure the tracker and apply to LoopBack interface and shut the tracker observe the NAT behviour	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.010	To configure Pool overload with destination Nat along fallback verify traffic validation.	Configure Pool overload with destination Nat along fallback verify traffic validation.	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.011	configure tracker in pool overload and verify Nat translations	Configure tracker in pool overload and apply to DIA interface and verify Nat translations	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.012	configure the DIA interface overload in the wan interface before destination Nat validate the traffic	Configure the DIA interface overload in the wan interface before destination Nat validate the traffic	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.013	Configure endpoint tracker for dns in wan interface with DIA interface overload	Configure to overload the DIA interface overload and attach the endpoint tracker with dns type track the traffic	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.014	To reload the c-edge device and check the Nat translation performance	Validate the NAT traffice and dest NAT before and after reloading the device	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.015	To configure the Destination Nat using v-manage cli template and check the performance.	To configure the Destination Nat using v-manage cli template and check the performance.	Passed	

ENJ.Des_Nat.20.11.1_17.11.1_N.016	To configure the destination Nat with multiple flow of vrf using device cli.	Create the multiple vrf in cli device and destination nat and verify the flow of traffic	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.017	Toflapping the DIA Interface and the check the traffic	Toflapping the DIA Interface and the check the traffic	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.018	Tocheck the traffic after flapping the overlay interface and enable fallback in policy.	Flapping the overlay interface and enable fallback in policy and check the traffic	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.019	To configure the Destination Nat interface overload in cat8k and check the performance.	Configure the Destination Nat interface overload in cat8k and check the performance.	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.020	To configure multiple entry to same destination nat translation should be blocked	Configure same destination nat translation with multiple entry should be blocked	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.021	To configure the destination Nat with dual tracker dia(boolean and)	Configure the destination Nat with dual tracker dia(boolean and)	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.022	To configure the destination Nat with dual tracker dia(boolean or)	Configure the destination Nat with dual tracker dia(boolean or) and apply to NAT interface	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.023	To remove the new knob destination Nat command and check their Nat translation functionality.	Remove the new knob destination Nat command and check their Nat translation functionality.	Passed	
ENJ.Des_Nat.20.11.1_17.11.1_N.024	To configure the source and destination match condition data policy in destination Nat and check the translation	Configure the source and destination match condition data policy in destination Nat and check the translation	Passed	

ENJ.Des_Nat.20.11.1_17.11.1_N.025	To configure the destination Nat and check the hardware data path.To configure the destination Nat and check the hardware data path.	Configure the destination Nat and check the hardware data path.	Passed	

NAT ALG Support

Logical ID	Title	Description	Status	Defect ID
ENJ. NAT_ALG_20.11.1_17.11.1_N.01	To enable the nat alg for pptp and generate the traffic and check the translation.	Configure the pptp after enable the nat alg and generate the traffic and check the translation.	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.02	To enable the nat alg for sunrpc tcp and generate the traffic and check the translation.	Configure the sunrpc tcp in interface after enable the nat alg and generate the traffic and check the translation.	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.03	To enable the nat alg for sunrpc udp and generate the traffic and check the translation.	Configure the sunrpc udp in interface after enable the nat alg and generate the traffic and check the translation.	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.04	To enable all the nat alg service and generate the traffic and check all the translation.	enable all the nat alg service and generate the traffic and check all the translation.	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.05	To configure the loopback interface with nat alg service for pptp protocol	To configure pptp protocol in the loopback interface with nat alg service check pptp traffic	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.06	To configure the dynamic inside for the nat and check the performance	Configure the dynamic nat inside for the nat alg service for pptp and check the performance.	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.07	To flapping the wan interface and check the performance of nat	Shut and unshut the wan interface and check the performance of nat	Passed	

ENJ. NAT_ALG_20.11.1_17.11.1_N.08	To configure the static inside for the nat and check the translation	Configure and Apply the pptp protocol with the static nat inside for the nat alg service and check the translation.	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.09	To configure the centralized data policy for vpn with nat alg specific service and check the translation.	Configure the centralized data policy for vpn with nat alg specific service and check the translation.	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.10	To configure the nat dia route within service vpn for nat alg service for tcp.	Configure tcp protocol the nat dia route within service vpn and enable nat alg service check traslation	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.11	To enable the two alg nat protocol and generate the traffic and check the translation.	Configure to enable the two alg nat protocol and generate the traffic and check the translation.	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.12	To reload the cEdge device and check the nat command and function are available.	Reload the cEdge device and check the nat command and function are available.	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.13	To configure the nat alg service for tftp using vmanage cli add on template.	Configure the nat alg service for tftp using vmanage cli add on template and apply to the cedge device	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.14	To configure the nat alg for pptp using vmanage cli add on template and check the translation.	Configure the nat alg for pptp using vmanage cli add on template and check the translation and apply to cdege device	Passed	

ENJ. NAT_ALG_20.11.1_17.11.1_N.15	To check the alg statistics after configure the sunrpc protocol with nat alg.	Configure the sunrpc protocol with nat alg and check the alg statistics	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.16	To enable the nat alg for tftp service then generate the traffic and check the translation.	Enable the nat alg for tftp service then generate the traffic and check the translation.	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.17	To clear a nat translation and recreate a session in client and verify alg function.	Configure recreate a session by clearing the nat translation in client and verify alg function.	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.18	To enable and disable the nat alg in client side and check the translation	Check nat behaviour by enable and disable the nat alg in client side and check the translation	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.19	To configure the pptp for ZBFW and check the alg function.	Configure the pptp for ZBFW and check the alg function.	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.20	To configure the nat alg for sunrpc using vmanage cli add on template and monitor the nat.	Configure the nat alg for sunrpc using vmanage cli add on template and monitor the nat and check the nat translations	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.21	To enable the nat alg for sccp and generate the traffic and check the translation.	Configure and enable the nat alg for sccp and generate the traffic and check the translation.	Passed	
ENJ. NAT_ALG_20.11.1_17.11.1_N.22	To enable the nat alg for h323 and generate the traffic and check the translation.	Configure and enable the nat alg for h323 and generate the traffic and check the translation.	Passed	

SDWAN CLI c8000V SDWAN Enterprise Certificate Support

Logical ID	Title	Description	Status	Defect ID
ENJ.C8k_20.11.1_17.11.1_N.01	Configure CAs License for c8000V SDWAN Enterprise	Configure CAs License for c8000V SDWAN Enterprise and verify	Passed	
ENJ.C8k_20.11.1_17.11.1_N.02	Check the Throughput and System Hardware Throttling	Check the Throughput and System Hardware Throttling Specifications in the Autonomous Mode or nots	Passed	
ENJ.C8k_20.11.1_17.11.1_N.03	Check the Throughput and System Hardware Throttling Specifications in the SD-WAN Controller Mode or not	Check the Throughput and System Hardware Throttling Specifications in the SD-WAN Controller Mode or not and verify	Passed	
ENJ.C8k_20.11.1_17.11.1_N.04	Configured a numeric throughput value on the device and the license PID is a numeric license and check tier-based throughput value converted or not	Configured a numeric throughput value on the device and the license PID is a numeric license and check tier-based throughput value converted or not and verify	Passed	
ENJ.C8k_20.11.1_17.11.1_N.05	Configure CAs Certificates and the current SD-WAN solution to validate each device and Verify On-boxing	Configure CAs Certificates and the current SD-WAN solution to validate each device and verify On-boxing	Passed	
ENJ.C8k_20.11.1_17.11.1_N.06	vManage-Signed certificate created and signed by vManage using its own created CA	Verify vManage-Signed certificate created and signed by vManage using its own created CA	Passed	

ENJ.C8k_20.11.1_17.11.1_N.07	Verify the licence should be Cisco PKI/Symantec-Signed or not	Check licence should be Cisco PKI/Symantec-Signed or not	Passed	
ENJ.C8k_20.11.1_17.11.1_N.08	Customer specific PKI support – available for both controllers and edge devices	Check the customer specific PKI support – available for both controllers and edge devices or not	Passed	
ENJ.C8k_20.11.1_17.11.1_N.09	Enterprise certificates support requires the ability to configure the organization name and verify	Enterprise certificates support requires the ability to configure the organization name and verify	Passed	
ENJ.C8k_20.11.1_17.11.1_N.10	Configuring the certificate organization name during CSR generation and Verify Certificate by default value	Configuring the certificate organization name during CSR generation and Verify Certificate by default value	Passed	
ENJ.C8k_20.11.1_17.11.1_N.11	Check the Only accepts properly formatting organization name should be string	Check the Only accepts properly formatting organization name should be string	Passed	
ENJ.C8k_20.11.1_17.11.1_N.12	Check the High Availability (HA) working fine or not	Check the High Availability (HA) working fine or not after Cas configured	Passed	
ENJ.C8k_20.11.1_17.11.1_N.13	Configuring the certificate check Network Management Working fine or not	Configuring the certificate check Network Management Working fine or not	Passed	
ENJ.C8k_20.11.1_17.11.1_N.14	Check Security AAA/IPSEC working fine or not	Configured a numeric throughput value on the device and the license PID is a numeric license and check tier-based throughput value converted or not	Passed	

ENJ.C8k_20.11.1_17.11.1_N.15	Configure CAs Certificates check the Security VPN/ACL/SSH/Tunnels working fine or not	Configure CAs Certificates check the Security VPN/ACL/SSH/Tunnels working fine or not	Passed	
ENJ.C8k_20.11.1_17.11.1_N.16	Configure CAs Certificates and check Third Party Applications (SDN/OnePK) working fine or not	Configure CAs Certificates and check Third Party Applications (SDN/OnePK) working fine or not	Passed	
ENJ.C8k_20.11.1_17.11.1_N.17	Configure CAs Certificates and check Quality of Service (QoS)	Configure CAs Certificates and check Quality of Service (QoS) and Verify	Passed	
ENJ.C8k_20.11.1_17.11.1_N.18	Configure CAs Certificates and check Multi-tenancy	Configuring CAs Certificates and check Multi-tenancy	Passed	
ENJ.C8k_20.11.1_17.11.1_N.19	Configure CAs Certificates and check the The cloud onramp is working or not	Configure CAs Certificates and check the The cloud onramp is working or not	Passed	
ENJ.C8k_20.11.1_17.11.1_N.20	Upgrade coordination between systems and check CAs Certificates	Upgrade coordination between systems and Verify CAs Certificates	Passed	

Regression Features

QoS

Logical ID	Title	Status	Defect ID
ENJ.QoS.20.11.1_17.11.1_N01	To monitor the data traffic using dscp value in QOS marking class map policy.	Passed	
ENJ.QoS.20.11.1_17.11.1_N02	To configure the LLQ with a priority percent for a single traffic	Passed	
ENJ.QoS.20.11.1_17.11.1_N03	To configure the LLq and CBWFQ with a multiple traffic of class map policy.	Passed	
ENJ.QoS.20.11.1_17.11.1_N04	To configure a single rate two color policing with cir 128kbpa for a single traffic	Passed	
ENJ.QoS.20.11.1_17.11.1_N05	To configure the two-rate policing with Cir 500kbps and peak rate of 1mbps.	Passed	
ENJ.QoS.20.11.1_17.11.1_N06	To configure a shaping on the bandwidth percent queues in a qos traffic	Passed	
ENJ.QoS.20.11.1_17.11.1_N07	To configure an average shaping range with 8000kbps	Passed	
ENJ.QoS.20.11.1_17.11.1_N08	To configure an adaptive shaping of upstream bandwidth range with 6000kbps	Passed	
ENJ.QoS.20.11.1_17.11.1_N09	To configure a bandwidth allocation based on data traffic in a queue	Passed	
ENJ.QoS.20.11.1_17.11.1_N10	To configure the queue limit allocation based on the traffic in queue (using WRED).	Passed	
ENJ.QoS.20.11.1_17.11.1_N11	To configure the Per-VPN QOS and generate the traffic and check the performance.	Passed	

ENJ.QoS.20.11.1_17.11.1_N12	To configure a knob of vm traffic forwarding class queue using cli.	Passed	
ENJ.QoS.20.11.1_17.11.1_N13	To delete the knob of vm traffic class of queue user choice and check the global attribute id using cli.	Passed	
ENJ.QoS.20.11.1_17.11.1_N14	To configure an adaptive shaping of downstream bandwidth range with 8000kbps.	Passed	
ENJ.QoS.20.11.1_17.11.1_N15	To configure the forwarding qos and generate the traffic using v-manage feature template.	Passed	

DIA

Logical ID	Title	Status	Defect ID
ENJ.DIA.20.11.1_17.11.1_N01	To configure the Service side outside dynamic NAT with centralized data policy.	Passed	
ENJ.DIA.20.11.1_17.11.1_N02	To configure the Service side outside dynamic NAT overload with data policy.	Passed	
ENJ.DIA.20.11.1_17.11.1_N03	To configure the inside static NAT using an Inside Nat pool using centralized policy.	Passed	
ENJ.DIA.20.11.1_17.11.1_N04	To configure the static inside NAT and static outside Nat mapped inside Nat address pool	Passed	
ENJ.DIA.20.11.1_17.11.1_N05	To configure a service side PAT port forwarding with inside tcp traffic(http-80) via CLI.	Passed	
ENJ.DIA.20.11.1_17.11.1_N06	To configure a service side static Nat port forwarding with inside tcp traffic(telnet-23) via CLI.	Passed	
ENJ.DIA.20.11.1_17.11.1_N07	To configure the intra vpn service side Nat and generate the traffic and check the translation.	Passed	
ENJ.DIA.20.11.1_17.11.1_N08	To configure the service side conditional static Nat with data policy using CLI.	Passed	
ENJ.DIA.20.11.1_17.11.1_N09	To configure the service side conditional Dynamic Nat with data policy using CLI.	Passed	
ENJ.DIA.20.11.1_17.11.1_N10	To configure the service side Network Nat with data policy using CLI.	Passed	

ENJ.DIA.20.11.1_17.11.1_N11	To configure the service side static Nat object tracker with Data policy using cli.	Passed	
ENJ.DIA.20.11.1_17.11.1_N12	To configure the service side static Nat object tracker with Data policy using cli addon Template	Passed	
ENJ.DIA.20.11.1_17.11.1_N13	To configure the intra vpn service side Nat and generate the traffic using cli add on template	Passed	
ENJ.DIA.20.11.1_17.11.1_N14	To configure the service side conditional static Nat with matched and unmatched data policy and check the translation.	Passed	
ENJ.DIA.20.11.1_17.11.1_N15	To configure the service side static NAT using feature template and check the Nat translation	Passed	

NAT

Logical ID	Title	Status	Defect ID
ENJ.NAT.20.11.1_17.11.1_N01	To configure the Service side outside dynamic NAT with centralized data policy.	Passed	
ENJ.NAT.20.11.1_17.11.1_N02	To configure the Service side outside dynamic NAT overload with data policy.	Passed	
ENJ.NAT.20.11.1_17.11.1_N03	To configure the inside static NAT using an Inside Nat pool using centralized policy.	Passed	
ENJ.NAT.20.11.1_17.11.1_N04	To configure the static inside NAT and static outside Nat mapped inside Nat address pool	Passed	
ENJ.NAT.20.11.1_17.11.1_N05	To configure a service side PAT port forwarding with inside tcp traffic(http-80) via CLI.	Passed	
ENJ.NAT.20.11.1_17.11.1_N06	To configure a service side static Nat port forwarding with inside tcp traffic(telnet-23) via CLI.	Passed	
ENJ.NAT.20.11.1_17.11.1_N07	To configure the intra vpn service side Nat and generate the traffic and check the translation.	Passed	
ENJ.NAT.20.11.1_17.11.1_N08	To configure the service side conditional static Nat with data policy using CLI.	Passed	
ENJ.NAT.20.11.1_17.11.1_N09	To configure the service side conditional Dynamic Nat with data policy using CLI.	Passed	
ENJ.NAT.20.11.1_17.11.1_N10	To configure the service side Network Nat with data policy using CLI.	Passed	

ENJ.NAT.20.11.1_17.11.1_N11	To configure the service side static Nat object tracker with Data policy using cli.	Passed	
ENJ.NAT.20.11.1_17.11.1_N12	To configure the service side static Nat object tracker with Data policy using cli addon Template	Passed	
ENJ.NAT.20.11.1_17.11.1_N13	To configure the intra vpn service side Nat and generate the traffic using cli add on template	Passed	
ENJ.NAT.20.11.1_17.11.1_N14	To configure the service side conditional static Nat with matched and unmatched data policy and check the translation.	Passed	
ENJ.NAT.20.11.1_17.11.1_N15	To configure the service side static NAT using feature template and check the Nat translation	Passed	

5_Tuple

Logical ID	Title	Status	Defect ID
ENJ.5Tuple.20.11.1_17.11.1_N01	Policy with Destination Data Prefix rule using vManage	Passed	
ENJ.5Tuple.20.11.1_17.11.1_N02	Policy with Destination port rule using vManage	Passed	
ENJ.5Tuple.20.11.1_17.11.1_N03	Policy with Protocol rule using vManage	Passed	
ENJ.5Tuple.20.11.1_17.11.1_N04	Policy with Source Data Prefix rule using vManage	Passed	
ENJ.5Tuple.20.11.1_17.11.1_N05	Policy with Source Port rule using vManage	Passed	
ENJ.5Tuple.20.11.1_17.11.1_N06	Policy with Destination Data Prefix rule using CLI	Passed	
ENJ.5Tuple.20.11.1_17.11.1_N07	Policy with Destination port rule using CLI	Passed	
ENJ.5Tuple.20.11.1_17.11.1_N08	Policy with Protocol rule using CLI	Passed	
ENJ.5Tuple.20.11.1_17.11.1_N09	Policy with Source Data Prefix rule using CLI	Passed	
ENJ.5Tuple.20.11.1_17.11.1_N10	Policy with Source port rule using CLI	Passed	

DPI

Logical ID	Title	Status	Defect ID
ENJ.DPI.20.11.1_17.11.1_N01	Basic Policy to drop and use counter for a DPI application family using vmanage	Passed	
ENJ.DPI.20.11.1_17.11.1_N02	Basic Policy to accept and use counter for a DPI application using vManage	Passed	
ENJ.DPI.20.11.1_17.11.1_N03	Policy to forward to a TLOC colour for the application family with failover using vmanage	Passed	
ENJ.DPI.20.11.1_17.11.1_N04	Policy to forward to a TLOC color for the application family without failover using vManage	Passed	
ENJ.DPI.20.11.1_17.11.1_N05	Basic Policy to drop and use counter for a DPI application family using CLI.	Passed	
ENJ.DPI.20.11.1_17.11.1_N06	Basic Policy to accept and use counter for a DPI application using CLI.	Passed	

AAR with custom

Logical ID	Title	Status	Defect ID
ENJ.AAR.20.11.1_17.11.1_N01	Basic Policy with Custom Application	Passed	
ENJ.AAR.20.11.1_17.11.1_N02	Policy with Custom Application with Server name, IP	Passed	
ENJ.AAR.20.11.1_17.11.1_N03	Policy with Custom Application with specified source IP and Port	Passed	
ENJ.AAR.20.11.1_17.11.1_N04	Policy with Custom Application with specified Server name and Ports	Passed	
ENJ.AAR.20.11.1_17.11.1_N05	Policy with Custom Application with specified source Ports and transport protocol(TCP/UDP)	Passed	
ENJ.AAR.20.11.1_17.11.1_N06	Color Preference and Count with Custom Application.	Passed	
ENJ.AAR.20.11.1_17.11.1_N07	SLA low-loss low-latency Policy with Custom Application	Passed	
ENJ.AAR.20.11.1_17.11.1_N08	SLA low-loss high-latency Policy with Custom Application	Passed	
ENJ.AAR.20.11.1_17.11.1_N09	SLA high-loss high-latency Policy with Custom Application	Passed	

C_Flowd

Logical ID	Title	Status	Defect ID
ENJ.CFlowd.20.11.1_17.11.1_N01	To Configure Cflowd Traffic Flow Monitoring Using the CLI	Passed	
ENJ.CFlowd.20.11.1_17.11.1_N02	To Configure Cflowd Traffic Flow Monitoring with ipv4-record using the CLI	Passed	
ENJ.CFlowd.20.11.1_17.11.1_N03	To Configure Cflowd Traffic Flow Monitoring Using vManage	Passed	
ENJ.CFlowd.20.11.1_17.11.1_N04	To Configure Cflowd Traffic Flow Monitoring with ipv4-records Using vManage	Passed	

Routing

Logical ID	Title	Status	Defect ID
ENJ.Routing.20.11.1_17.11.1_N01	EBGP configs on the transport side.	Passed	
ENJ.Routing.20.11.1_17.11.1_N02	Configure EBGP on the transport side using keepalive & hold time	Passed	
ENJ.Routing.20.11.1_17.11.1_N03	Decreasing Convergence by BFD configuration for BGP	Passed	
ENJ.Routing.20.11.1_17.11.1_N04	To Configure the EBGP on the loopback address on the CEdge and verify the Routes.	Passed	
ENJ.Routing.20.11.1_17.11.1_N05	EBGP neighborship with Weight preference Between MPLS and Wan Edge router in Branch	Passed	
ENJ.Routing.20.11.1_17.11.1_N06	To configure BGP Service side to WAN Edge for VRF 100	Passed	
ENJ.Routing.20.11.1_17.11.1_N07	EBGP neighborship with Local Preference Between MPLS and Wan Edge router in Branch	Passed	
ENJ.Routing.20.11.1_17.11.1_N08	To configure and verify the sub interface in the CEDGE router with VLAN 802.1Q in the Transport side	Passed	
ENJ.Routing.20.11.1_17.11.1_N09	To establish ibgp peer between CEDGE Router 1 and Edge Router 2 alone side Service router with the BGP timers 30 and 90 Sec Keep alive and the Hold timers	Passed	
ENJ.Routing.20.11.1_17.11.1_N10	To configure the Fixed IP in the Gigabit Ethernet interface on the Router	Passed	

ENJ.Routing.20.11.1_17.11.1_N11	Configure Speed as Auto on 2 neighbouring Interfaces and verify the Link is up	Passed	
ENJ.Routing.20.11.1_17.11.1_N12	Configure Duplex as Half on 2 Interfaces and Verify the Link is up	Passed	
ENJ.Routing.20.11.1_17.11.1_N13	Configure Auto and Full Duplex on 2 neighbouring Interfaces and Verify the Link	Passed	
ENJ.Routing.20.11.1_17.11.1_N14	Static route with different next hops using preference value on Service side	Passed	
ENJ.Routing.20.11.1_17.11.1_N15	To Configure and verify the Static route with the link Failure	Passed	

VPN_Segmentation

Logical ID	Title	Status	Defect ID
ENJ.VPN.20.11.1_17.11.1_N01	Configure VRF Segmentation Using the CLI (VRF100 VRF200)	Passed	
ENJ.VPN.20.11.1_17.11.1_N02	To configure BGP Service side to WAN Edge for VRF 100	Passed	
ENJ.VPN.20.11.1_17.11.1_N03	To configure OSPF Service side to WAN Edge for VRF 100	Passed	
ENJ.VPN.20.11.1_17.11.1_N04	To configure EIGRP Service side to WAN Edge for VRF 100	Passed	
ENJ.VPN.20.11.1_17.11.1_N05	To Advertise and redistribute the OMP routes for VRF 100	Passed	

VRRP

Logical ID	Title	Status	Defect ID
ENJ.VRRP20.11.1_17.11.1_N01	Active/Standby VRRP on c-Edge Routers	Passed	
ENJ.VRRP20.11.1_17.11.1_N02	Configure failover on Active/Standby router and Master takes back the role of master when it comes up again from down state using VRRP on cEdge routers to provide redundancy.	Passed	
ENJ.VRRP20.11.1_17.11.1_N03	Pre-empt enabled on Failover to Active/Standby router in VRRP.	Passed	
ENJ.VRRP20.11.1_17.11.1_N04	Disable Pre-empt on Failover to an Active/Standby router in VRRP	Passed	
ENJ.VRRP20.11.1_17.11.1_N05	Active/Active VRRP on cEdge routers	Passed	
ENJ.VRRP20.11.1_17.11.1_N06	Failover on Active/Active VRRP on cEdge router.	Passed	
ENJ.VRRP20.11.1_17.11.1_N07	Pre-empt enabled on Failover to Active/Active router in VRRP	Passed	
ENJ.VRRP20.11.1_17.11.1_N08	Disable Pre-empt on Failover to Active/Active router in VRRP	Passed	
ENJ.VRRP20.11.1_17.11.1_N09	Configure Multiple VRRP Groups on the Same LAN Interface	Passed	
ENJ.VRRP20.11.1_17.11.1_N10	VRRP Overlay Management Protocol (OMP) Tracking	Passed	

Adhoc

Logical ID	Title	Title Description	Status	Defect ID
ENJ.SDWAN_20.11.1_17.11.1_N01	To successfully generate a App Route Visualization traffic from a remote device.	When the App Route Visualization generation is unsuccessfull, Seems the page is getting freezed and can't able to change the fields.	Failed	CSCwf00050
ENJ.SDWAN_20.11.1_17.11.1_N02	To create a TAC Case in SCM Wizard Tool.	When user navigate into Tools > Tac Cases, to open a case in the page there is an option SCM Wizard, so when user tries to scroll down the page it isn't working	Failed	CSCwf08143
ENJ.SDWAN_20.11.1_17.11.1_N03	Tagging Edge Devies based on the Lab Setup Environment	When user is tagging edge devices based on their respective lab setup environment the tags are not getting assigned properly & happening rogue tag assignation.	Failed	CSCwf01714
ENJ.SDWAN_20.11.1_17.11.1_N04	Generating the Admin Tech log Files.	when user tries to download the Admin-Tech file, so the operational command of Admin-Tech is misleading to download the files.	Failed	CSCwf01664

ENJ.SDWAN_20.11.1_17.11.1_N05	To Monitor App Route Visualization Page.	When we navigate into monitoring the App Route Visualization page, the path which is visible is irrelevant and if we click the path it is redirecting to some other unknown page.	Failed	CSCwf01687
ENJ.SDWAN_20.11.1_17.11.1_N06	Check the Integration Management using ISE to Add connection	Check the Add connection option in ISE and verify the same	Failed	CSCwe63882
ENJ.SDWAN_20.11.1_17.11.1_N07	To check the credentials for PMT in Administration Settings page	When we navigate into Administration Settings page in Vmanage and check to PMT credentials password by Eye button , the password is not visible	Failed	CSCwf09775
ENJ.SDWAN_20.11.1_17.11.1_N08	To check the credentials for PMT in Administration Settings page	When we navigate into Administration Settings page in Vmanage and check to PMT credentials, its enabled by wrong Client ID and wrong Client Secret	Failed	CSCwf09720
ENJ.SDWAN_20.11.1_17.11.1_N09	To check the View/close button for Sig credentials in Administration Settings page	When we navigate into Administration Settings page in Vmanage and check to "View/close" button for Sig credentials, But close button is missing	Failed	CSCwf09126

ENJ.SDWAN_20.11.1_17.11.1_N10	To check the Sig credentials Setting in Administration Settings page	When we navigate into Administration Settings page in Vmanage and check to Sig credentials Setting, its enabled by wrong Org-id ,wrong Api-key, wrong api-secret	Failed	CSCwf08136
ENJ.SDWAN_20.11.1_17.11.1_N11	To check the credentials for Smart account in Administration Settings page	When we navigate into Administration Settings page in Vmanage and check to Smart account password by Eye button , the password is not visible	Failed	CSCwf08075
ENJ.SDWAN_20.11.1_17.11.1_N12	To check the credentials for Smart account in Administration Settings page	When we navigate into Administration Settings page in Vmanage and check to Smart account, its enabled by wrong User Name,Wrong Password	Failed	CSCwf08046
ENJ.SDWAN_20.11.1_17.11.1_N13	To check the Enterprise CA in Administration Settings page	When we navigate into Administration Settings page in Vmanage check the Enterprise CA is Successfully Authorized in Administration setting But its not Display Authorized	Failed	CSCwe82284

ENJ.SDWAN_20.11.1_17.11.1_N14	To check whether the Add Feature Profile is displayed in Configuration Group	When we try to Add policy object profile/feature profile the page itself is not getting displayed/broken once we get into it.	Failed	CSCwf00174

Related Documents

Related Documentation

Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release 17.11 Release Notes

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/17-11/sd-wan-rel-notes-xe-17-11.html

Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.11

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 NAT Configuration Guide, Cisco IOS XE Release 17.11

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/nat/nat-book-xe-sdwan/configure-nat.html#nat-direct-internet-access

Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.11

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/centralized-policy.html#id_107620

Cisco SD-WAN Monitor and Maintain Configuration Guide,Cisco IOS XE Release 17.11

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/m-dashboard-screen.html#monitor-security

Cisco SD-WAN Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.11

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

Cisco SD-WAN Security Configuration Guide, Cisco IOS XE Release 17.11

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