Test Results Summary for IOS XE SD-WAN for Japan (Release Version 20.10.1/17.10.1)

First Published: 2023-01-31

Last Modified: 2023-02-16

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 20.10.1 - IOS XE 17.10.1
- 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

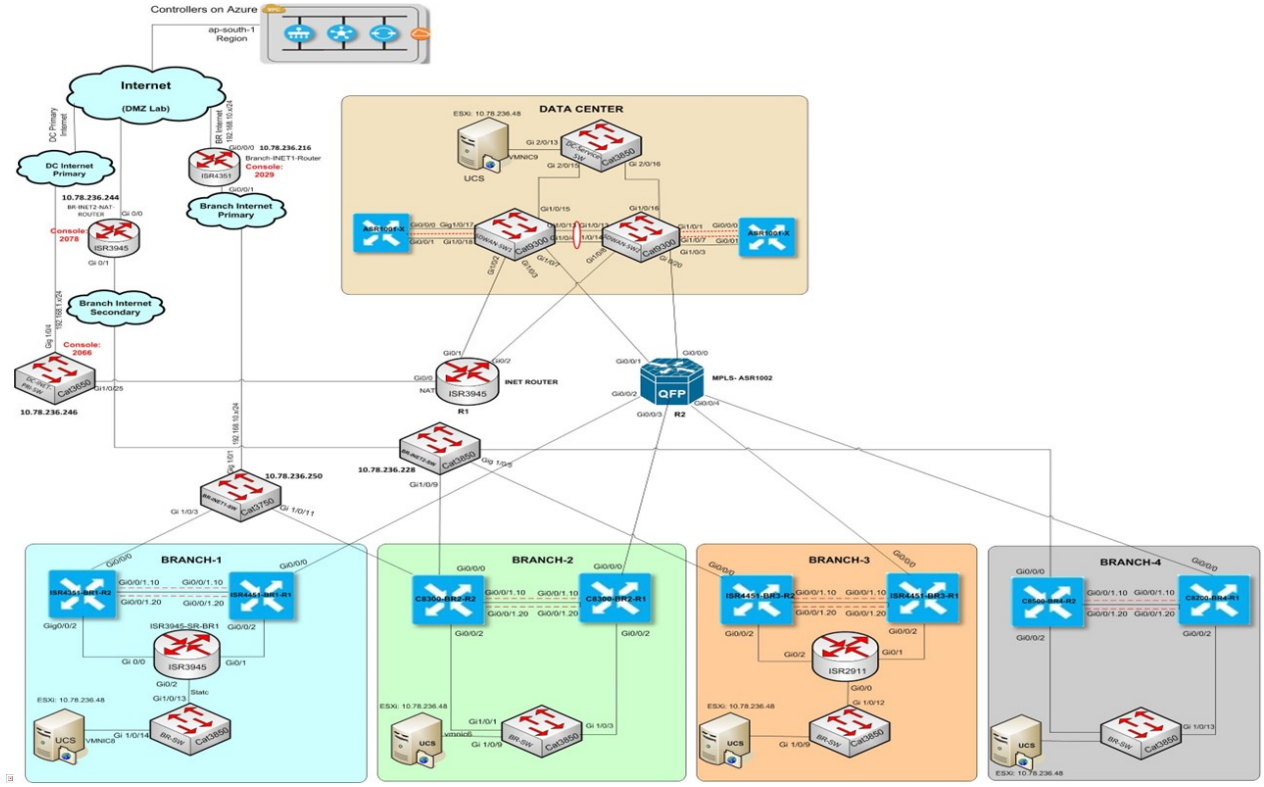
Acronym	Description
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AF	Address-family
API	Application Programming Interface
ASN	Autonomous System Number
ASR	Aggregation Services Routers
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BR	Branch
BR Site	Branch 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	20.10.1
		vManage	20.10.1
		vSmart	20.10.1
	Switch	Cat 9K PoE	17.2
Communications Infrastructure	IOS XE SDWAN	C8300, C8200 & C8500L	17.10.1
		ISR4461	17.10.1
UCS	UCSC-C240-M5SX	ESXi Host	6.0, 6.5
Client	Operating System	End point	Windows 10
	Browsers	Mozilla	109.0
		Chrome	105.0. 5195.127

What's New ?

SDWAN 20.10.1 - IOS XE 17.10.1 Solution testing

- SDWAN UX 2.0 - Configuration, Monitoring, Reporting and Troubleshooting
- SD-WAN identity-based firewall(phase-2) - SGT and pxcloud integration
- Pinning applications to best performing WAN Links under adverse WAN Conditions
- vManage be able to integrate with multiple IDPs(Azure AD)
- SD-WAN Application classification 2.0
- IPS Custom Signature and offline updates
- Ability to configure source port preservation for known BFD ports
- [cEdge] FNF Enhancements to export BFD/AAR telemetry
- Hierarchical SD-WAN - 4th phase
- Support Webex Telemetry within Cloud onRamp - SaaS

Open Caveats

CDETS ID	Title
CSCwd89012	Tested flap-based auto-suspension - Minimum duration value - no results as expected
CSCwd97646	PUT /sdavc/cloudconnector not Disabling Telemetry
CSCwe11554	Unused System IP Pool subnet cannot be deleted
CSCwd91652	Unable to access device cli mode When we attach template of Internet Secure getway
CSCwe01210	When SD-AVC cloud connector is Enabled to Disabled then Enabled Why OTP is getting Error
CSCwe15673	sig Tunnel interface is down in active-active states
CSCwe14276	Unable to Enabled Webex Application on onramp for Saas in Cloud Vmanage_20.10.1
CSCwe16600	Can't Able to Self Ping in the vManage UI
CSCwe16604	Refusing the inbetween range for MTU in Dialer interface
CSCwd80969	Log/Alarm - Not able to drag the scroll bar
CSCwd93298	Allowing to create view with empty character values under SNMP feature in configuration group
CSCwe00441	Rule ID for accounting parcel under system profile is not visible in vManage UI
CSCwd06485	In snmp-server user configuration remote keyword is not accepting
CSCwe01573	In T-Loc Interface the Ports aren't Preserving after configuring the CLI Knob Command.
CSCwe17436	In vManage UI, the selected paths were wrongly displayed & buttons were not working properly.
CSCwe17674	In vManage UI, Select Device -> Speed Test & in that the settings button some options were missing
CSCwe17692	In vManage UI,Select Device -> Speed Test & in that the settings Icon is having Functionality issue
CSCwe16660	Can't Able to Set Custom Time & Also displaying a Wrong Error Log.
CSCwd93319	Allowing to create Key type with empty space under AAA local user
CSCwe13114	Allowing to create Segment Name with empty space under LAN & Service VPN Profile

CSCwe16676	Allowing ppp chap password string 0 but showing password as string 7 in Dailer
CSCwe16459	NAT DIA Tracker to support interval period upto 10 seconds
CSCwd90479	Best path ECMP not working unless subregion configured on Transport Gateway Border Router
CSCwd89400	Administrator->Settings->options IDP is not functioning properly - UI Issue
CSCwd81081	To add report Id under My reports and Task completed status
CSCwe17712	Need to add APP QOE and Zscaler, Tunnel health,statistics settings under administration setting
CSCwe01198	SD-AVC Cloud connector When enabled in Vmanage ,its not display Enabled in Administration Settings

Resolved Caveats

CDETS ID	Title
CSCwd79974	Device Cannot connect to the SD-AVC network service with Default Config
CSCwd70666	Reenabling SDAVC is not handled
CSCwd70941	Issue in asssociate/disassociate the sub feature under profiles in configuration group
CSCwd87508	SGT bindings and User group pxgrid bindings are not reflected to vsmarts when they are in cluster
CSCwe13117	Tunnel periodicity values is accepting beyond the maximum value
CSCwd93254	Document Updation for AAA
CSCwe05229	Document Updation for Transport and management profile
CSCwe00642	Document Updation SDWAN UX 2.0 Configuration 2.0,Feature Profiles & Configuration Groups
CSCwd93145	Document Updation tracker parcel

New Features

SDWAN UX 2-0 - Configuration, Monitoring, Reporting and Troubleshooting

Logical ID	Title	Description	Status	Defect ID
ENJ.UX2.020.10.1_17.10.1_N.01	To enable and edit the execute summary report	To enable and edit the execute summary report	Passed	
ENJ.UX2.020.10.1_17.10.1_N.02	To check executive summary report for site health	To check executive summary report for site health	Passed	
ENJ.UX2.020.10.1_17.10.1_N.03	To delete the report from "Executive Report Preview" after report generated	To delete the report from "Executive Report Preview" after report generated	Passed	
ENJ.UX2.020.10.1_17.10.1_N.04	To download the report in PDF and verify the generated reports includes all parameters	To download the report in PDF and verify the generated reports includes all parameters	Passed	
ENJ.UX2.020.10.1_17.10.1_N.05	To Generate multiple reports and check in My Reports tabs for all the available reports	To Generate multiple reports and check in My Reports tabs for all the available reports	Passed	
ENJ.UX2.020.10.1_17.10.1_N.06	To Filter the data based on schedule type, status, and time range on report summary	To Filter the data based on schedule type, status, and time range on report summary	Passed	
ENJ.UX2.020.10.1_17.10.1_N.07	To verify preview of report is available using hyperlink	To verify preview of report is available using hyperlink	Passed	
ENJ.UX2.020.10.1_17.10.1_N.08	To enable alarm notification to send the report along with address	To enable alarm notification to send the report along with address	Passed	
ENJ.UX2.020.10.1_17.10.1_N.09	To check and verify the available tools in the troubleshooting option	To check and verify the available tools in the troubleshooting option	Passed	

ENJ.UX2.020.10.1_17.10.1_N.10	To perform packer capture under site topology	To perform packer capture under site topology	Passed	
ENJ.UX2.020.10.1_17.10.1_N.11	To verify the underlay traffic using tunnel table	To verify the underlay traffic using tunnel table	Passed	
ENJ.UX2.020.10.1_17.10.1_N.12	To monitor the tunnel health using tunnel table	To monitor the tunnel health using tunnel table	Passed	
ENJ.UX2.020.10.1_17.10.1_N.13	To monitor the app-route visualization using application table via path view	To monitor the app-route visualization using application table via path view	Passed	
ENJ.UX2.020.10.1_17.10.1_N.14	To add IPV4 ACL parcel in configuration group for match condition any any	To add IPV4 ACL parcel in configuration group for match condition any any	Passed	
ENJ.UX2.020.10.1_17.10.1_N.15	To allow ACL in single LAN interface under service profile in the configuration group with direction in and out	To allow ACL in single LAN interface under service profile in the configuration group with direction in and out	Passed	
ENJ.UX2.020.10.1_17.10.1_N.16	To allow ACL in single WAN interface under transport profile in the configuration group with direction in and out	To allow ACL in single WAN interface under transport profile in the configuration group with direction in and out	Passed	
ENJ.UX2.020.10.1_17.10.1_N.17	To Associate/Disassociate route policy from BGP/OSPF parcel	To Associate/Disassociate route policy from BGP/OSPF parcel	Passed	
ENJ.UX2.020.10.1_17.10.1_N.18	To add Tags (OMP/OSPF) in route policy using configuration group.	To add Tags (OMP/OSPF) in route policy using configuration group.	Passed	
ENJ.UX2.020.10.1_17.10.1_N.19	To add metrics in route policy using configuration group.	To add metrics in route policy using configuration group.	Passed	

ENJ.UX2.020.10.1_17.10.1_N.20	To create configuration group using cli add on profile	To create configuration group using cli add on profile	Passed	
ENJ.UX2.020.10.1_17.10.1_N.21	To create QOS parcel under service profile	To create QOS parcel under service profile	Passed	
ENJ.UX2.020.10.1_17.10.1_N.22	To create Route policy with Action - accept/deny option	To create Route policy with Action - accept/deny option	Passed	
ENJ.UX2.020.10.1_17.10.1_N.23	To check all application performance for single site using table/heat map view	To check all application performance for single site using table/heat map view	Passed	
ENJ.UX2.020.10.1_17.10.1_N.24	To delete the report using API	To delete the report using API	Passed	
ENJ.UX2.020.10.1_17.10.1_N.25	To create AAR policy with custom application	To create AAR policy with custom application	Failed	CSCwd79021
ENJ.UX2.020.10.1_17.10.1_N.26	To create centralized policy using API	To create centralized policy using API	Passed	
ENJ.UX2.020.10.1_17.10.1_N.27	To create localized policy using API	To create localized policy using API	Passed	
ENJ.UX2.020.10.1_17.10.1_N.28	To add Umbrella SIG parcel under configuration group	To add Umbrella SIG parcel under configuration group	Passed	
ENJ.UX2.020.10.1_17.10.1_N.29	To download report using API	To download report using API	Passed	
ENJ.UX2.020.10.1_17.10.1_N.30	To create a security policy under configuration group	To create a security policy under configuration group	Passed	
ENJ.UX2.020.10.1_17.10.1_N.31	To add SIG parcel for Zscaler and Generic SIG parcel under configuration group	To add SIG parcel for Zscaler and Generic SIG parcel under configuration group	Passed	
ENJ.UX2.020.10.1_17.10.1_N.32	To add performance monitor parcel under configuration group	To add performance monitor parcel under configuration group	Passed	

SD-WAN identity-based firewall-phase-2 - SGT and pxcloud integration

Logical ID	Title	Description	Status	Defect ID
ENJIDF20.10.1_17.10.1_N01	To integrate ISE with vManage by enabling pxGrid cloud (VPN 0) with SGT subscription	To integrate ISE with vManage by enabling pxGrid cloud (VPN 0) with SGT subscription	Passed	
ENJIDF20.10.1_17.10.1_N02	To check the ISE behaviour by integrating ISE with VPN 412	To check the ISE behaviour by integrating ISE with VPN 412	Passed	
ENJIDF20.10.1_17.10.1_N03	To retrieve SGT via ISE integration in vmanage	To retrieve SGT via ISE integration in vmanage	Passed	
ENJIDF20.10.1_17.10.1_N04	To Verify the behaviour when vManage losses connection to ISE	To Verify the behaviour when vManage losses connection to ISE	Passed	
ENJIDF20.10.1_17.10.1_N05	To verify the behavior when pxgrid account is disabled from ISE	To verify the behavior when pxgrid account is disabled from ISE	Passed	
ENJIDF20.10.1_17.10.1_N06	To create basic security policy with SGT	To create basic security policy with SGT	Passed	
ENJIDF20.10.1_17.10.1_N07	To allow the SGT group(10-Employye) to access cisco.com	To allow the SGT group(10-Employye) to access cisco.com	Passed	
ENJIDF20.10.1_17.10.1_N08	To block SGT group(partners - 20)to access youtube.com	To block SGT group(partners - 20)to access youtube.com	Passed	
ENJIDF20.10.1_17.10.1_N09	To allow specific user from employee to access youtube.com with SGT	To allow specific user from employee to access youtube.com with SGT	Passed	
ENJIDF20.10.1_17.10.1_N10	To check the IP SGT mapping on vmanage	To check the IP SGT mapping on vmanage	Passed	

ENJ.IDF.20.10.1_17.10.1_N11	To define unified security policy under NG firewall, add rule with source as SGT list	To define unified security policy under NG firewall, add rule with source as SGT list	Passed	
ENJ.IDF.20.10.1_17.10.1_N12	To define unified secuirty policy under NG firewall add rule with destination as SGT list	To define unified secuirty policy under NG firewall add rule with destination as SGT list	Passed	
ENJ.IDF.20.10.1_17.10.1_N13	To create MAX of 17 SGT's and check it can be configured under single identity list	To create MAX of 17 SGT's and check it can be configured under single identity list	Passed	
ENJ.IDF.20.10.1_17.10.1_N14	To check the behavior when FW policy has no SGT based rule, but SGT mapping is there on device.	To check the behavior when FW policy has no SGT based rule, but SGT mapping is there on device.	Passed	
ENJ.IDF.20.10.1_17.10.1_N15	To check the behaviour when both IP-based and SGT identity-based rules for same IP	To check the behaviour when both IP-based and SGT identity-based rules for same IP	Passed	
ENJ.IDF.20.10.1_17.10.1_N16	To check the SDWAN control connection after clearing ISE connections on Vmanage and Vsmarts	To check the SDWAN control connection after clearing ISE connections on Vmanage and Vsmarts	Passed	
ENJ.IDF.20.10.1_17.10.1_N17	To Check the behavior when IDMgr on vSmart restarts	To Check the behavior when IDMgr on vSmart restarts	Passed	
ENJ.IDF.20.10.1_17.10.1_N18	To Edit SGT-IP mapping with add/delete/modify option in the created firewall rule	To Edit SGT-IP mapping with add/delete/modify option in the created firewall rule	Passed	

ENJIDF20.10.1_17.10.1_N19	To integrate ISE with vManage by enabling pxGrid cloud (VPN 0) without SGT	To integrate ISE with vManage by enabling pxGrid cloud (VPN 0) without SGT	Passed	
ENJIDF20.10.1_17.10.1_N20	To Change the settings from user/user group otption to SGT and verify the results on ISE connections	To Change the settings from user/user group otption to SGT and verify the results on ISE connections	Passed	
ENJIDF20.10.1_17.10.1_N21	To Create identity based policy with sgt in identity-list along with other FW attributes	To Create identity based policy with sgt in identity-list along with other FW attributes	Passed	
ENJIDF20.10.1_17.10.1_N22	To delete the ISE connection from vManage with fw identity list and policy configured	To delete the ISE connection from vManage with fw identity list and policy configured	Passed	
ENJIDF20.10.1_17.10.1_N23	To delete the ISE connection from vmanage when no security policy and SGT configured	To delete the ISE connection from vmanage when no security policy and SGT configured	Passed	
ENJIDF20.10.1_17.10.1_N24	To Test newly added cli for SGT mappings, configs and stats then check user status for SGT on vSmart	To Test newly added cli for SGT mappings, configs and stats then check user status for SGT on vSmart	Passed	
ENJIDF20.10.1_17.10.1_N25	To check whether multiple SGT list can be configured per firewall in one direction	To check whether multiple SGT list can be configured per firewall in one direction	Failed	CSCwd99726
ENJIDF20.10.1_17.10.1_N26	To check the Events and alarms for ISE connections in vmanage	To check the Events and alarms for ISE connections in vmanage	Passed	
ENJIDF20.10.1_17.10.1_N27	To check whether multiple SGT list can be configured per firewall in one direction	To check whether multiple SGT list can be configured per firewall in one direction	Passed	

ENJ.IDF.20.10.1_17.10.1_N28	To check the behavior when FW policy has no SGT based rule, but SGT mapping is there on device	To check the behavior when FW policy has no SGT based rule, but SGT mapping is there on device	Passed	

Pinning applications to best performing WAN Links under adverse WAN Conditions

Logical ID	Title	Description	Status	Defect ID
ENJ.SP.20.10.1_17.10.1_N01	Configure & verify only auto-suspend and commit	Enable auto-suspend of session	Passed	
ENJ.SP.20.10.1_17.10.1_N02	Configure & verify no auto-suspend and commit	Disable auto-suspend of session	Passed	
ENJ.SP.20.10.1_17.10.1_N03	Configure SLA based auto suspension for the Wan Tunnel using CLI	Verify SLA based auto suspension	Passed	
ENJ.SP.20.10.1_17.10.1_N04	Verify the bfd session is suspended any alarm notification is send to vManage with flag	Verify auto suspension alarm notification send to vManage with flag	Passed	
ENJ.SP.20.10.1_17.10.1_N05	Validate bfd circuit will not send traffic during bfd session SLA based suspension	Verify no traffic is send during SLA based suspension of sessions	Passed	
ENJ.SP.20.10.1_17.10.1_N06	Validate the reset command for auto-suspend	Verify the bfd session for flap based suspension using timers	Passed	
ENJ.SP.20.10.1_17.10.1_N07	Validate the bfd session suspension timer reset & session moved to suspension list whenthe session flap doesn’t meet the SLA	Verify the bfd session for flap based suspension using timers with SLA	Passed	
ENJ.SP.20.10.1_17.10.1_N08	Verify bfd session when LR is configured	Verify Last resort value configured in auto suspension	Passed	

ENJ.SP.20.10.1_17.10.1_N09	Verify bfd session when LR is not configured	Verify Last resort value is not configured in auto suspension	Passed	
ENJ.SP.20.10.1_17.10.1_N10	Verify reboot or interface events are not included in the bfd events	Verify reboot/interface events not included in bfd events	Passed	
ENJ.SP.20.10.1_17.10.1_N11	Check the duration of time for which the session will be suspended using default value	Verify duration of time for flap based auto suspension using default values	Passed	
ENJ.SP.20.10.1_17.10.1_N12	Check the duration of time for which the session will be suspended using random value	Verify duration of time for flap based auto suspension using random values	Failed	CSCwd89012
ENJ.SP.20.10.1_17.10.1_N13	Check the number of flap after which the session will be suspended using default value	Verify number of flaps for flap based auto suspension using default values	Passed	
ENJ.SP.20.10.1_17.10.1_N14	Check the number of flap after which the session will be suspended using random value	Verify number of flaps for flap based auto suspension using random values	Passed	
ENJ.SP.20.10.1_17.10.1_N15	Check the detection of time within which the flapping of session needs to be detected with default value	Verify detection of time within which the flapping of session needs to be detected with default value	Passed	
ENJ.SP.20.10.1_17.10.1_N16	Check the detection of time within which the flapping of session needs to be detected with random value	Verify detection of time within which the flapping of session needs to be detected with random value	Passed	
ENJ.SP.20.10.1_17.10.1_N17	Set the local color on which threshold will apply/select all	Verify local color with apply all colors	Passed	

ENJ.SP.20.10.1_17.10.1_N18	Set the local color on which threshold will apply/select specific color	Verify local color with apply specific color	Passed	
ENJ.SP.20.10.1_17.10.1_N19	Configure Flap based auto suspension for the Wan Tunnel using vManage Device CLI template	Verify Flap based auto suspension for the Wan Tunnel using vManage Device CLI template	Passed	
ENJ.SP.20.10.1_17.10.1_N20	Configure SLA based auto suspension for the Wan Tunnel using vManage Device CLI template	Verify SLA based auto suspension for the Wan Tunnel using vManage Device CLI template	Passed	
ENJ.SP.20.10.1_17.10.1_N21	No Command for color Configuration 1. no thresholds / no color to Remove complete threshold block	Verify SLA based auto suspension for the Wan Tunnel using criteria	Passed	
ENJ.SP.20.10.1_17.10.1_N22	No Command for color Configuration 2. no thresholds color All to Remove All under threshold	Verify SLA based auto suspension for the Wan Tunnel using criteria	Passed	
ENJ.SP.20.10.1_17.10.1_N23	No Command for color Configuration 3. no thresholds color local-color to Remove all local-colors	Verify SLA based auto suspension for the Wan Tunnel using criteria	Passed	
ENJ.SP.20.10.1_17.10.1_N24	No Command for color Configuration 4. no thresholds color local-color <> to Remove specified local color	Verify SLA based auto suspension for the Wan Tunnel using criteria	Passed	
ENJ.SP.20.10.1_17.10.1_N25	Change one or few of the parameter values for an already configured color (loss,latency or jitter)	Verify SLA based auto suspension for the Wan Tunnel using criteria	Passed	

vManage be able to integrate with multiple IDPs Azure AD

Logical ID	Title	Description	Status	Defect ID
ENJ.IDP.20.10.1_17.10.1_N.01	Configure Azure AD using Vmanage	Configure Azure AD using Vmanage	Passed	
ENJ.IDP.20.10.1_17.10.1_N.02	Configure Azure AD Connect and sync Vmanage AD users to Azure AD	Configure Azure AD Connect and sync Vmanage AD users to Azure AD	Passed	
ENJ.IDP.20.10.1_17.10.1_N.03	Test Azure AD users sync from Vmanage	Test Azure AD users sync from Vmanage	Passed	
ENJ.IDP.20.10.1_17.10.1_N.04	Configure SSO on vmanage with Azure IDP and Sync the Azure AD users	Configure SSO on vmanage with Azure IDP and Sync the Azure AD users	Passed	
ENJ.IDP.20.10.1_17.10.1_N.05	Configure IDP with single domain name using vmanage	Configure IDP with single domain name using vmanage	Passed	
ENJ.IDP.20.10.1_17.10.1_N.06	Configure IDP by adding meta data before adding domain name and check the accessed users	Configure IDP by adding meta data before adding domain name and check the accessed users	Passed	
ENJ.IDP.20.10.1_17.10.1_N.07	Configure IDP with multiple email Domain names and authenticating through same IDP using vmanage	Configure IDP with multiple email Domain names and authenticating through same IDP using vmanage	Passed	
ENJ.IDP.20.10.1_17.10.1_N.08	Try to Configure email Domain name already mapped to Existing IDP and Check the Accessibility	Try to Configure email Domain name already mapped to Existing IDP and Check the Accessibility	Passed	
ENJ.IDP.20.10.1_17.10.1_N.09	Configure Two IDPs with same IDP names and verify Whether it is accepting or not	Configure Two IDPs with same IDP names and verify Whether it is accepting or not	Passed	

ENJ.IDP.20.10.1_17.10.1_N.10	Modify the existing IDP without changing the email domain names and check the authenticated Users	Modify the existing IDP without changing the email domain names and check the authenticated Users	Passed	
ENJ.IDP.20.10.1_17.10.1_N.11	Configure another IDP without adding the metada in IDP section & add domain names and check users are able to Authenticate	Configure another IDP without adding the metada in IDP section & add domain names and check users are able to Authenticate	Passed	
ENJ.IDP.20.10.1_17.10.1_N.12	Disable and Enable one IDP and check the Authentication Performance	Disable and Enable one IDP and check the Authentication Performance	Passed	
ENJ.IDP.20.10.1_17.10.1_N.13	To Delete Specific email domain name from IDP and check the User Access	To Delete Specific email domain name from IDP and check the User Access	Passed	
ENJ.IDP.20.10.1_17.10.1_N.14	Try to add the email domain name to existing IDP , Which is availble in Disabled IDP and check the particular domain getting access or not	Try to add the email domain name to existing IDP , Which is availble in Disabled IDP and check the particular domain getting access or not	Passed	
ENJ.IDP.20.10.1_17.10.1_N.15	Verify the View option in Identity provided setting to check the created IDP name, state & domain names available	Verify the View option in Identity provided setting to check the created IDP name, state & domain names available	Passed	
ENJ.IDP.20.10.1_17.10.1_N.16	Verify the Edit option in Identity provided setting to check the Edit IDP name, state & domain names available	Verify the Edit option in Identity provided setting to check the Edit IDP name, state & domain names available	Passed	
ENJ.IDP.20.10.1_17.10.1_N.17	Changes to add, edit, disable and enable IdPs will be logged to audit log	Changes to add, edit, disable and enable IdPs will be logged to audit log	Passed	

ENJ.IDP.20.10.1_17.10.1_N.18	Configure maximum of 3 IDP & verify the max limit with out XML file	Configure maximum of 3 IDP & verify the max limit with out XML file	Passed	
ENJ.IDP.20.10.1_17.10.1_N.19	We can delete any IdP of the three and we should be able to add another IdP	We can delete any IdP of the three and we should be able to add another IdP	Passed	
ENJ.IDP.20.10.1_17.10.1_N.20	Configure IDP by adding random inactive domain name and check the whether it get accessed	Configure IDP by adding random inactive domain name and check the whether it get accessed	Passed	
ENJ.IDP.20.10.1_17.10.1_N.21	Configure IDP OKTA domain name and check the whether it get accessed	Configure IDP OKTA domain name and check the whether it get accessed	Passed	
ENJ.IDP.20.10.1_17.10.1_N.22	Configure IDP PING domain name and check the whether it get accessed	Configure IDP PING domain name and check the whether it get accessed	Passed	
ENJ.IDP.20.10.1_17.10.1_N.23	Configure 3 IDP with domain name and check whether it get accessed	Configure 3 IDP with domain name and check whether it get accessed	Passed	

SD-WAN Application classification 2-0

Logical ID	Title	Description	Status	Defect ID
ENJ.AppClass.20.10.1_17.10.1_N.01	Cluster with SDAVC on one VM enables Gateway on other VMs	Cluster with SDAVC on one VM enables Gateway on other VMs	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.02	Cluster with SDAVC enables service on one VM alone	Cluster with SDAVC enables service on one VM alone	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.03	Verify Cloud connector is removed from vManage	Verify Cloud connector is removed from vManage	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.04	Verify SDAVC service has SDAVC SAAS and Cloud connector in vManage	Verify SDAVC service has SDAVC SAAS and Cloud connector in vManage	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.05	SDAVC with SAAS enabled	SDAVC with SAAS enabled	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.06	SDAVC with SAAS disabled	SDAVC with SAAS disabled	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.07	SDAVC without cloud connect	SDAVC without cloud connect	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.08	Verify OTP with SDAVC service from vManage	Verify OTP with SDAVC service from vManage	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.09	SDAVC with cloud connect and Telemetry	SDAVC with cloud connect and Telemetry	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.10	Verify cloud connector is reflected when enabled after SDAVC	Verify cloud connector is reflected when enabled after SDAVC	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.11	SDAVC with cloud connect and no Telemetry	SDAVC with cloud connect and no Telemetry	Passed	

ENJ.AppClass.20.10.1_17.10.1_N.12	Adding custom apps with SDAVC on the service VM	Adding custom apps with SDAVC on the service VM	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.13	Removing custom apps with SDAVC	Removing custom apps with SDAVC	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.14	Verify SDAVC custom apps are not displayed on different VM	Verify SDAVC custom apps are not displayed on different VM	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.15	SDAVC with AAR	SDAVC with AAR	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.16	SDAVC with cloud connector and AAR	SDAVC with cloud connector and AAR	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.17	SDAVC with SAAS and AAR	SDAVC with SAAS and AAR	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.18	SDAVC with data policy	SDAVC with data policy	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.19	Manually start SDAVC agent on VM	Manually start SDAVC agent on VM	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.20	Manually stop SDAVC agent on VM	Manually stop SDAVC agent on VM	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.21	CurrentCloudConfig API	CurrentCloudConfig API	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.22	Disable Cloud API	Disable Cloud API	Failed	CSCwd96314,CSCwd97646
ENJ.AppClass.20.10.1_17.10.1_N.23	RemoveCredentials API	RemoveCredentials API	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.24	Get Cloud Status API	Get Cloud Status API	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.25	SDAVC app rules API	SDAVC app rules API	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.26	Create applications to verify they’re reflected on Edge device with SDAVC Network Service blocked	Create applications to verify they’re reflected on Edge device with SDAVC Network Service blocked	Passed	
ENJ.AppClass.20.10.1_17.10.1_N.27	AAR with SDAVC Network Service blocked	AAR with SDAVC Network Service blocked	Passed	

ENJ.AppClass.20.10.1_17.10.1_N.28	Data Policy with SDAVC Network Service blocked	Data Policy with SDAVC Network Service blocked	Passed	

IPS Custom Signature and offline updates

Logical ID	Title	Description	Status	Defect ID
ENJ.IPS.20.10.1_17.10.1_N.01	Configure the IPS Custom Signature via vmanage feature template.	Configure the IPS Custom Signature via vmanage feature template.	Passed	
ENJ.IPS.20.10.1_17.10.1_N.02	To configure the Ips custom signature policy via cli.	To configure the Ips custom signature policy via cli.	Passed	
ENJ.IPS.20.10.1_17.10.1_N.03	To delete the Ips policy and check the signature log	To delete the Ips policy and check the signature log	Passed	
ENJ.IPS.20.10.1_17.10.1_N.04	To configure the custom signature with a alert level Alert syslog and check.	To configure the custom signature with a alert level Alert syslog and check.	Passed	
ENJ.IPS.20.10.1_17.10.1_N.05	To add the customer signature file with existing code in the utd with a default signature file.	To add the customer signature file with existing code in the utd with a default signature file.	Passed	
ENJ.IPS.20.10.1_17.10.1_N.06	To configure the IPS Custom Signature with a detection mode	To configure the IPS Custom Signature with a detection mode	Passed	
ENJ.IPS.20.10.1_17.10.1_N.07	To configure the balanced customer signature set and check the performance	To configure the balanced customer signature set and check the performance	Passed	
ENJ.IPS.20.10.1_17.10.1_N.08	To reboot cEdge to see the custom signature rules still exit in the device	To reboot cEdge to see the custom signature rules still exit in the device	Passed	
ENJ.IPS.20.10.1_17.10.1_N.09	To remove UTD custom signature from vmanage and check the performance.	To remove UTD custom signature from vmanage and check the performance.	Passed	

ENJ.IPS.20.10.1_17.10.1_N.10	To reboot UTD container to see the custom signature rules still exit in the device	To reboot UTD container to see the custom signature rules still exit in the device	Passed	
ENJ.IPS.20.10.1_17.10.1_N.11	To SDWAN clear control connections in the cEdge device while the save action is in progress for the custom signature	To SDWAN clear control connections in the cEdge device while the save action is in progress for the custom signature	Passed	
ENJ.IPS.20.10.1_17.10.1_N.12	To UTD switch to remote sever for custom IPS	To UTD switch to remote sever for custom IPS	Passed	
ENJ.IPS.20.10.1_17.10.1_N.13	To use UTD toggle save button after security policy is attached to the device	To use UTD toggle save button after security policy is attached to the device	Passed	
ENJ.IPS.20.10.1_17.10.1_N.14	To reinstall the UTD container with custom IPS and offline signature	To reinstall the UTD container with custom IPS and offline signature	Passed	
ENJ.IPS.20.10.1_17.10.1_N.15	To configure ips along with threat protection	To configure ips along with threat protection	Passed	
ENJ.IPS.20.10.1_17.10.1_N.16	To define custom signature by using utd with zbfw	To define custom signature by using utd with zbfw	Passed	
ENJ.IPS.20.10.1_17.10.1_N.17	To define custom signature with utd with url	To define custom signature with utd with url	Passed	
ENJ.IPS.20.10.1_17.10.1_N.18	To define custom signature utd with application	To define custom signature utd with application	Passed	
ENJ.IPS.20.10.1_17.10.1_N.19	To define IPS custom signature to allow the particular URL with url filtering	To define IPS custom signature to allow the particular URL with url filtering	Passed	
ENJ.IPS.20.10.1_17.10.1_N.20	To define IPS custom signature to block the particular URL with URL filtering	To define IPS custom signature to block the particular URL with URL filtering	Passed	

ENJ.IPS.20.10.1_17.10.1_N.21	To update UTD signature on Vmanage	To update UTD signature on Vmanage	Passed	
ENJ.IPS.20.10.1_17.10.1_N.22	To change the UTD interval from default and verify the results on UTD signature update	To change the UTD interval from default and verify the results on UTD signature update	Passed	
ENJ.IPS.20.10.1_17.10.1_N.23	To check whether vmanage generates global custom signature	To check whether vmanage generates global custom signature	Passed	
ENJ.IPS.20.10.1_17.10.1_N.24	To use offline signature update and check the performance	To use offline signature update and check the performance	Passed	
ENJ.IPS.20.10.1_17.10.1_N.25	To use ips without target vpn the profile gets download or not and to check the performance	To use ips without target vpn the profile gets download or not and to check the performance	Passed	
ENJ.IPS.20.10.1_17.10.1_N.26	To monitor the intrusion prevention policy in vmanage.	To monitor the intrusion prevention policy in vmanage.	Passed	

Ability to configure source port preservation for known BFD ports

Logical ID	Title	Description	Status	Defect ID
ENJ.BFD_20.10.1_17.10.1_N.01	Configure the BFD Port preservation with UDP port range	By using to configure the range of UDP protocol in BFD port preservation	Failed	CSCwd88003
ENJ.BFD_20.10.1_17.10.1_N.02	Configure the BFD Preservation with the TLOC extension	Configuration to preserve source ports by establish TLOC extension	Passed	
ENJ.BFD_20.10.1_17.10.1_N.03	Configure the DIA NAT interface overload with BFD source Port	To configure the BFD source port with DIA NAT interface overload	Passed	
ENJ.BFD_20.10.1_17.10.1_N.04	Configure the BFD port preservation with DIA interface overload	By using cli knob we have to configure BFD port preservation with DIA interface overload	Passed	
ENJ.BFD_20.10.1_17.10.1_N.05	Configure Pool with ip addresses range in the same subnet as DIA interface	By using pool configuration with ip address range in same subnet as DIA interface	Passed	
ENJ.BFD_20.10.1_17.10.1_N.06	Configure the BFD Port preservation with cli KNOB command	Configure the BFD Port preservation with cli KNOB command	Passed	
ENJ.BFD_20.10.1_17.10.1_N.07	Configure the particular UDP Range with BFD port preservation	Able to configure the particular range of UDP port along with BFD	Passed	
ENJ.BFD_20.10.1_17.10.1_N.08	Configure to enable the source port preservation during nat translation	Enable the source port preservation during NAT translation	Passed	

ENJ.BFD_20.10.1_17.10.1_N.09	To configure port preservation configuration with DIA interface	By using port preservation configuration need to check the nat translation	Passed	
ENJ.BFD_20.10.1_17.10.1_N.10	Configure the NAT DIA interface and check the BFD ports without Cli KNOB	Configure the NAT DIA interface and check the BFD ports without Cli KNOB	Passed	
ENJ.BFD_20.10.1_17.10.1_N.11	Ability to configure the port preservation with NAT translation in interface overload	By using Nat translation to configure port preservation in one of the interface	Passed	
ENJ.BFD_20.10.1_17.10.1_N.12	Configure the BFD port with ip nat outside along with DIA interface overload	By using BFD port to configure the ip nat outside along with DIA interface	Passed	
ENJ.BFD_20.10.1_17.10.1_N.13	Configure BFD port preservation during DIA Pool overload (different subnet)	By using cli knob we have to configure BFD port preservation with DIA pool overload by using different subnets	Passed	
ENJ.BFD_20.10.1_17.10.1_N.14	Configure the DIA pool in same subnet with port preservation along egress interface	By using cli knob we have to configure BFD port preservation with DIA pool overload	Passed	
ENJ.BFD_20.10.1_17.10.1_N.15	Configure to enable the Cli KNOB with IP NAT inside to verify NAT translations	By using cli knob we have to configure BFD port preservation with IP NAT inside and verify NAT translations	Passed	
ENJ.BFD_20.10.1_17.10.1_N.16	Configuration after KNOB command to check the NAT translation	Configuration after KNOB command to check the NAT translation	Passed	

ENJBFD_20.10.1_17.10.1_N.17	Configure befor KNOB command to check the NAT translation along with BFD table	By using cli knob we have to configure BFD port preservation with IP NAT inside and verify NAT translations	Passed	
ENJBFD_20.10.1_17.10.1_N.18	Configure to shut the DIA interface and check the ability of BFD and NAT	Shutting the DIA interface port and checking the bfd and nat translations	Passed	
ENJBFD_20.10.1_17.10.1_N.19	After reload the Device and check the BFD port preservation and NAT configurations	Reloading the DUT device and check source port presevation	Passed	
ENJBFD_20.10.1_17.10.1_N.20	Configure to readd the existing NAT after adding the "ip nat setting preserve-sdwan-ports". and check the performance	Remove and re add the nat configuration check the bfd preservation	Passed	
ENJBFD_20.10.1_17.10.1_N.21	Configure source port preservation in UUT through cli template using vManage.	By using source port preservation in under Device through CLI template	Passed	
ENJBFD_20.10.1_17.10.1_N.22	Configure to Flap DIA Interface (T-LOC) and verify & Validate the flow of BFD table and NAT Translations.	Configure to Flap DIA Interface (T-LOC) and verify & Validate the flow of BFD table and NAT Translations.	Failed	CSCwe01573 , CSCwe01746
ENJBFD_20.10.1_17.10.1_N.23	Configure Source Port Preservation for DIA Interface Overload Using a CLI Template	Configure Source Port Preservation for DIA Interface Overload Using a CLI Template	Passed	
ENJBFD_20.10.1_17.10.1_N.24	Configure Source Port Preservation for DIA Pool Overload Using a CLI Template	Configure Source Port Preservation for DIA Pool Overload Using a CLI Template	Passed	

ENJBFD_20.10.1_17.10.1_N25	Configure Source Port Preservation for DIA Loopback Overload Using a CLI Template	Configure Source Port Preservation for DIA Loopback Overload Using a CLI Template	Passed	

cEdge FNF Enhancements to export BFD-AAR telemetry

Logical ID	Title	Description	Status	Defect ID
ENJ.FNF.20.10.1_17.10.1_N.01	To configure the FNF ENC with bfd metrics via vmanage features template	To configure the FNF ENC with bfd metrics via vmanage features template	Passed	
ENJ.FNF.20.10.1_17.10.1_N.02	To configure the FNF ENC with bfd metrics via CLI template.	To configure the FNF ENC with bfd metrics via CLI template.	Passed	
ENJ.FNF.20.10.1_17.10.1_N.03	To disable the bfd metrics and check the functionality.	To disable the bfd metrics and check the functionality.	Passed	
ENJ.FNF.20.10.1_17.10.1_N.04	To refresh the time interval in bfd metrics and check the performance	To refresh the time interval in bfd metrics and check the performance	Passed	
ENJ.FNF.20.10.1_17.10.1_N.05	To check the behaviors with flapping the bfd session	To check the behaviors with flapping the bfd session	Passed	
ENJ.FNF.20.10.1_17.10.1_N.06	To change the bfd metric values and validate in CLI	To change the bfd metric values and validate in CLI	Passed	
ENJ.FNF.20.10.1_17.10.1_N.07	To configure the FNF ENC with bfd metrics vmanage centralized policy	To configure the FNF ENC with bfd metrics vmanage centralized policy	Passed	
ENJ.FNF.20.10.1_17.10.1_N.08	To verify the bfd exporting data for multiple BFD colour.	To verify the bfd exporting data for multiple BFD colour.	Passed	
ENJ.FNF.20.10.1_17.10.1_N.09	To change and verify the MTU size and the FNF Bfd behavior.	To change and verify the MTU size and the FNF Bfd behavior.	Passed	
ENJ.FNF.20.10.1_17.10.1_N.10	To configure the IPFIX Export in the FNF ENC with bfd metrics	To configure the IPFIX Export in the FNF ENC with bfd metrics	Passed	

ENJ.FNF.20.10.1_17.10.1_N.11	To configure the SNMP-walk with enable bfd metrics and check.	To configure the SNMP-walk with enable bfd metrics and check.	Passed	
ENJ.FNF.20.10.1_17.10.1_N.12	To configure the SNMP-walk with disable bfd metrics and check	To configure the SNMP-walk with disable bfd metrics and check	Passed	
ENJ.FNF.20.10.1_17.10.1_N.13	To configure and check the bfd metrics with tloc-tabls	To configure and check the bfd metrics with tloc-tabls	Passed	
ENJ.FNF.20.10.1_17.10.1_N.14	To configure the bfd metrics and flapping the interface and check the behavior	To configure the bfd metrics and flapping the interface and check the behavior	Passed	
ENJ.FNF.20.10.1_17.10.1_N.15	To configure the bfd metric and check the performance via vmanage	To configure the bfd metric and check the performance via vmanage	Passed	
ENJ.FNF.20.10.1_17.10.1_N.16	To configure the AAR with custom application and verify the bfd metric values.	To configure the AAR with custom application and verify the bfd metric values.	Passed	
ENJ.FNF.20.10.1_17.10.1_N.17	To check the bfd metrics with enabling and disabling the app-visibility.	To check the bfd metrics with enabling and disabling the app-visibility.	Passed	
ENJ.FNF.20.10.1_17.10.1_N.18	To configure the AAR SLA CLASS and check the bfd metrics.	To configure the AAR SLA CLASS and check the bfd metrics.	Passed	
ENJ.FNF.20.10.1_17.10.1_N.19	To disable the export spreading and enable the bfd metrics along with the interval and check the behaviors.	To disable the export spreading and enable the bfd metrics along with the interval and check the behaviors.	Passed	

ENJ.FNF.20.10.1_17.10.1_N.20	To configure the FNF for udp transport protocol with a bfd metrics value.	To configure the FNF for udp transport protocol with a bfd metrics value.	Passed	

Hierarchical SD-WAN - 4th phase

Logical ID	Title	Description	Status	Defect ID
ENJ.HSDWAN.20.10.1_17.10.1_N.01	Configure and verify subregions	Configure and verify subregions	Passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.02	Verify inability to configure subregion 0	Verify inability to configure subregion 0	Passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.03	Verify ability to add 63 subregions	Verify ability to add 63 subregions	Passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.04	Associating Region with different subregion	Associating Region with different subregion	Passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.05	Shutting OMP with subregions	Shutting OMP with subregions	Passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.06	Delete subregions and check it's reflected	Delete subregions and check it's reflected	Passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.07	Policy match with any-access	Policy match with any-access	Passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.08	Policy match with core	Policy match with core	Passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.09	Policy match with subregions	Policy match with subregions	Passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.10	Best-path Preference with subregion	Best-path Preference with subregion	Passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.11	Best-path ECMP with subregion	Best-path ECMP with subregion	Failed	CSCwd90479
ENJ.HSDWAN.20.10.1_17.10.1_N.12	Ribout caching with outbound policy	Ribout caching with outbound policy	Passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.13	Verify Ribout caching not applied with non-outbound policy	Verify Ribout caching not applied with non-outbound policy	Passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.14	Verify Ribout caching changes when policy is changed	Verify Ribout caching changes when policy is changed	Passed	

ENJHSDWAN20.10.1_17.10.1_N.15	Verify policy without Ribout caching	Verify policy without Ribout caching	Passed	
ENJHSDWAN20.10.1_17.10.1_N.16	Verify subregion association with core-region	Verify subregion association with core-region	Passed	
ENJHSDWAN20.10.1_17.10.1_N.17	Verify subregion association with secondary-region	Verify subregion association with secondary-region	Passed	
ENJHSDWAN20.10.1_17.10.1_N.18	Subregions with BR	Subregions with BR	Passed	
ENJHSDWAN20.10.1_17.10.1_N.19	Subregions with BR failover	Subregions with BR failover	Passed	
ENJHSDWAN20.10.1_17.10.1_N.20	Subregions with transport gateway	Subregions with transport gateway	Passed	
ENJHSDWAN20.10.1_17.10.1_N.21	Best-path Preference with site type cloud	Best-path Preference with site type cloud	Passed	
ENJHSDWAN20.10.1_17.10.1_N.22	Best-path ECMP with site type br	Best-path ECMP with site type br	Passed	
ENJHSDWAN20.10.1_17.10.1_N.23	Best-path Preference with site type type-1	Best-path Preference with site type type-2	Passed	
ENJHSDWAN20.10.1_17.10.1_N.24	Best-path ECMP with site type type-2	Best-path ECMP with site type type-3	Passed	
ENJHSDWAN20.10.1_17.10.1_N.25	Best-path Preference with site type type-3	Best-path Preference with site type type-4	Passed	

Support Webex Telemetry within Cloud onRamp - SaaS

Logical ID	Title	Description	Status	Defect ID
ENJ.Saas.20.10.1_17.10.1_N.01	Single branch single edge having dual DIA link & we are configuring CoR SAAS and enable O365/Webex Telemetry (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in dual DIA and DIA-1 having drops or latency switchover the traffic via DIA-2 & confirm the exit interfaces as an SIG auto tunnel interface.	Failed	CSCwd18826, CSCwd20426
ENJ.Saas.20.10.1_17.10.1_N.02	Single branch single edge having dual DIA link & we are configuring CoR SAAS and the internet exit point as a SIG automatic tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in dual DIA and DIA-1 having drops or latency switchover the traffic via DIA-2 & confirm the exit interfaces as an SIG auto tunnel interface	Passed	
ENJ.Saas.20.10.1_17.10.1_N.03	Single branch single edge having dual GW site link & we are configuring CoR SAAS and the internet exit point as a SIG automatic tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in dual GW site and GW-1 having drops or latency switchover the traffic via GW-2 & confirm the exit interfaces as an SIG auto tunnel interface.	Passed	

ENJ.Saas.20.10.1_17.10.1_N.04	Single branch single edge having one DIA link & one GW site link & we are configuring CoR SAAS and the internet exit point as a SIG automatic tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in one DIA & GW link, if DIA-1 having drops or latency switchover the traffic via GW & confirm the exit interfaces as an SIG auto tunnel interface.	Passed	
ENJ.Saas.20.10.1_17.10.1_N.05	Single branch single edge having one DIA link & one SWG link & we are configuring CoR SAAS and the internet exit point as a SIG automatic tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in one DIA and SWG, if DIA having drops or latency switchover the traffic via SWG & confirm the exit interfaces as an SIG auto tunnel interface.	Passed	
ENJ.Saas.20.10.1_17.10.1_N.06	Single branch single edge having one GW site link & one SWG link & we are configuring CoR SAAS and the internet exit point as a SIG automatic tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in one GW and SWG, if GW-link having drops or latency switchover the traffic via SWG & confirm the exit interfaces as an SIG auto tunnel interface.	Passed	

ENJ.Saas.20.10.1_17.10.1_N.07	Single branch single edge having one DIA link and one GW site link & one SWG link & we are configuring CoR SAAS and the internet exit point as a SIG automatic tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in one DIA & GW & SWG, if DIA having drops or latency switchover the traffic to remaining links based on vQoE value & confirm the exit interfaces as an SIG auto tunnel interface.	Passed	
ENJ.Saas.20.10.1_17.10.1_N.08	Single branch single edge having one DIA link & one GW site link & we are configuring CoR SAAS and the internet exit point as a SIG Manual tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in one DIA and one GW, if DIA having drops or latency switchover the traffic via GW & confirm the exit interfaces as an SIG Manual tunnel interface.	Passed	
ENJ.Saas.20.10.1_17.10.1_N.09	Single branch single edge having Dual DIA link & we are configuring CoR SAAS and the internet exit point as a SIG Manual tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in dual DIA and DIA-1 having drops or latency switchover the traffic via DIA-2 & confirm the exit interfaces as an SIG Manual tunnel interface.	Passed	

ENJ.Saas.20.10.1_17.10.1_N.10	Single branch single edge having dual GW site link & we are configuring CoR SAAS and the internet exit point as a SIG Manual tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in dual GW and GW-1 having drops or latency switchover the traffic via GW-2 & confirm the exit interfaces as an SIG Manual tunnel interface.	Passed	
ENJ.Saas.20.10.1_17.10.1_N.11	Single branch single edge having one DIA link & one SWG link & we are configuring CoR SAAS and the internet exit point as a SIG Manual tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in one DIA & one SWG, if DIA having drops or latency switchover the traffic via SWG & confirm the exit interfaces as an SIG Manual tunnel interface.	Passed	
ENJ.Saas.20.10.1_17.10.1_N.12	Single branch single edge having one GW site link & one SWG link & we are configuring CoR SAAS and the internet exit point as a SIG Manual tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in one GW and SWG, if GW having drops or latency switchover the traffic via SWG & confirm the exit interfaces as an SIG Manual tunnel interface.	Passed	

ENJ.Saas.20.10.1_17.10.1_N.13	Single branch single edge having one DIA link and one GW site link & one SWG link & we are configuring CoR SAAS and the internet exit point as a SIG Manual tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in one DIA & GW & SWG. If DIA having drops or latency switchover the traffic via remaining links based on vQoE values & confirm the exit interfaces as an SIG Manual tunnel interface.	Passed	
ENJ.Saas.20.10.1_17.10.1_N.14	Single branch dual edge having dual DIA link & we are configuring CoR SAAS and the internet exit point as a SIG automatic tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in dual DIA in dual node, if node-1 DIA having drops or latency switchover the traffic node-2 DIA & confirm the exit interfaces as an SIG auto tunnel interface.	Passed	
ENJ.Saas.20.10.1_17.10.1_N.15	Single branch dual edge having single DIA link and single GW site & we are configuring CoR SAAS and the internet exit point as a SIG automatic tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in dual node having DIA and GW, if node-1 DIA having drops or latency switchover the traffic via node-2 GW & confirm the exit interfaces as an SIG auto tunnel interface.	Passed	

ENJ.Saas.20.10.1_17.10.1_N.16	Single branch dual edge having dual DIA link & we are configuring CoR SAAS and the internet exit point as a SIG manual tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in dual edge having dual DIA and node-1 DIA having drops or latency switchover the traffic via node-2 DIA & confirm the exit interfaces as an SIG Manual tunnel interface.	Passed	
ENJ.Saas.20.10.1_17.10.1_N.17	Single branch dual edge having single DIA link and single GW site & we are configuring CoR SAAS and the internet exit point as a SIG manual tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in single branch dual node, if node-1 DIA having drops or latency switchover the traffic via node-2 GW & confirm the exit interfaces as an SIG auto tunnel interface.	Passed	
ENJ.Saas.20.10.1_17.10.1_N.18	Single branch dual edge having single DIA link and single SWG site & we are configuring CoR SAAS and the internet exit point as a SIG manual tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify in single branch dual node, if node-1 DIA having drops or latency switchover the traffic via node-2 SWG & confirm the exit interfaces as an SIG auto tunnel interface.	Passed	

ENJ.Saas.20.10.1_17.10.1_N.19	Single branch single edge having dual SWG link & we are configuring CoR SAAS and the internet exit point as a SIG automatic tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS).	Verify if branch SWG-1 having drops or latency switchover the traffic via SWG-2 & confirm the exit interfaces as an SIG auto tunnel interface	Passed	
ENJ.Saas.20.10.1_17.10.1_N.20	Single branch dual edge having single DIA link and single GW site & we are configuring CoR SAAS and the internet exit point as a SIG manual tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS)	Single branch dual edge having single DIA link and single GW site & we are configuring CoR SAAS and the internet exit point as a SIG manual tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS)	Passed	
ENJ.Saas.20.10.1_17.10.1_N.21	Single branch dual edge having single DIA link and single SWG site & we are configuring CoR SAAS and the internet exit point as a SIG manual tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS)	Single branch dual edge having single DIA link and single SWG site & we are configuring CoR SAAS and the internet exit point as a SIG manual tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS)	Passed	

ENJ.Saas.20.10.1_17.10.1_N.22	Single branch single edge having dual SWG link & we are configuring CoR SAAS and the internet exit point as a SIG automatic tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS)	Single branch single edge having dual SWG link & we are configuring CoR SAAS and the internet exit point as a SIG automatic tunnel interface (Support Webex Telemetry within Cloud onRamp - SaaS)	Passed	
ENJ.Saas.20.10.1_17.10.1_N.23	Connect SD-AVC cloud connector and opt-in webex telemetry in saas application and check by Vanalystic (Support Webex Telemetry within Cloud onRamp - SaaS)	Connect SD-AVC cloud connector and opt-in webex telemetry in saas application and check by Vanalystic (Support Webex Telemetry within Cloud onRamp - SaaS)	Passed	
ENJ.Saas.20.10.1_17.10.1_N.24	Connect SD-AVC cloud connector and opt-out webex telemetry in saas application and check by Vanalystic (Support Webex Telemetry within Cloud onRamp - SaaS)	Connect SD-AVC cloud connector and opt-out webex telemetry in saas application and check by Vanalystic (Support Webex Telemetry within Cloud onRamp - SaaS)	Passed	
ENJ.Saas.20.10.1_17.10.1_N.25	Connect SD-AVC cloud connector and opt-in webex telemetry in saas application and check by Vanalystic all region active or not (Support Webex Telemetry within Cloud onRamp - SaaS)	Connect SD-AVC cloud connector and opt-in webex telemetry in saas application and check by Vanalystic all region active or not (Support Webex Telemetry within Cloud onRamp - SaaS)	Passed	

Regression Features

Hierarchical SD-WAN - 3rd phase

Logical ID	Title	Status	Defect ID
ENJ.HSDWAN.20.10.1_17.10.1_N.01	Configure and validate Secondary Region ID for an Edge Router Using CLI	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.02	Configure the Secondary Region Mode to handle only Secondary Region traffic Using VManage	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.03	Configure the Secondary Region Mode to handle traffic in the primary and secondary regions using vManage	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.04	Configure a Device to Use Both the Primary-Region Path and Secondary-Region Path Using VManage	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.05	Configure Transport Gateway with ECMP Using vManage	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.06	Configure Transport Gateway with ECMP Using vManage and bring down a Transport Gateway	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.07	Configure Transport Gateway with ECMP Using CLI	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.08	Without a direct path, configure Transport Gateway with preference Using vManage	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.09	With a direct path, configure Transport Gateway with preference Using vManage	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.10	With a direct path, configure Transport Gateway with preference Using CLI	passed	

ENJ.HSDWAN.20.10.1_17.10.1_N.11	With a direct path, configure Transport Gateway with preference Using vManage and bring down the Transport Gateway	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.12	Configure Transport Gateway on multiple devices within the same region and verify that re-originated route is not advertised to another transport gateway	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.13	Configure an Affinity Group and Preference on a Device, Using vManage	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.14	Configure an Affinity Group and Preference to achieve Load Balancing for Access Region Traffic to Border Routers	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.15	Configure an Affinity Group and Preference with Only Paths in the Affinity Preference List	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.16	Configure an Affinity Group and Preference to achieve Load Balancing for Access Region Traffic to Edge Routers	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.17	Configure an Affinity Group and Preference to achieve Load Balancing for Core Region Traffic	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.18	Configure an Affinity Group, Preference, and affinity-preference outbound enable	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.19	Brownfield Migration to with new HSDWAN migration mode using vManage	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.20	Configure Migration mode from BGP Core using VManage	passed	

ENJ.HSDWAN.20.10.1_17.10.1_N.21	Configure a Application Route Policy for Edge router Matching Traffic-To, Region and Role	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.22	Configure a Application Route Policy for Border router Matching Traffic-To, Region and Role	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.23	Configure a Application Route Policy for Border router Matching Traffic-To, Region and Role Using Cisco vManage	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.24	Create preferred color group list for region	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.25	Configure Route Preference based on TLOC color and Path Type	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.26	Configure Control Policy to Match Traffic-To Using vManage	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.27	Match Traffic According to the Destination Region Using CLI	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.28	Configure the Path Preference for a Preferred Color Group List in a Data Policy	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.29	With a direct path, configure Transport Gateway with preference Using vManage and test Re-Origination Dampening under 10 seconds	passed	
ENJ.HSDWAN.20.10.1_17.10.1_N.30	With a direct path, configure Transport Gateway with preference Using vManage and test Re-Origination Dampening over 10 seconds	passed	

SIG Tunnel Monitoring -Observability for Zscaler -Umbrella Services

Logical ID	Title	Status	Defect ID
ENJ.SIGTM.20.10.1_17.10.1_N.01	Verify the enhanced visibility fields (HA pair, Provider, tracker, etc) with cEdge as compared to vEdge	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.02	Change the Tunnel ID for Tunnel and verify the change is reflected under new visibility field	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.03	Change the Site ID for Tunnel and verify the change is reflected under new visibility	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.04	Enable Tracker for Tunnel and verify the change is reflected under new visibility field	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.05	Disable Tracker for Tunnel and verify the change is reflected under new visibility field	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.06	Configure Destination Data center for Tunnel and verify it is displayed under new visibility field	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.07	Change the Destination Data center for Tunnel and verify the change is reflected under new visibility field	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.08	Configure Active-Active SIG Tunnel and verify HA Pair shows as active	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.09	Configure Active-Active SIG Tunnel, change it to Active-Backup and verify HA Pair shows as backup	Passed	

ENJ.SIGTM.20.10.1_17.10.1_N.10	Configure Active-Backup SIG Tunnel and verify HA Pair shows as backup Pair shows as backup	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.11	Configure Active-Backup SIG Tunnel, change it to Active-Active and verify	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.12	Configure Source-Only Load sharing enabled SIG Tunnel and verify	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.13	Configure Weighted SIG Active-Active Source-Only Load Sharing and verify	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.14	Configure Active-Backup SIG and verify Tunnel state is Up/Color is Green	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.15	Without Tracker enabled, bring down Active Tunnel and verify Tunnel state is still Up/ Color is still Green	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.16	Without Tracker enabled, bring down Active and Backup Tunnels and verify Tunnel State is Down/Color is Red	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.17	Bring down a Tracker, then verify Tunnel state is Down/Color is Orange, Tunnel Event details and counts	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.18	Bring up a downed Tracker and verify Tunnel state is Down/Color is Green and Tunnel Event details	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.19	Under Top Application over SIG, verify the Top Applications are displayed as expected	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.20	Change usage of Top Applications, verify the Top Applications are changed	Passed	

ENJ.SIGTM.20.10.1_17.10.1_N.21	Shut the backup tunnel and check the tunnel traffic and status with verify the change is reflected under new visibility field	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.22	Shut the active tunnel and check the tunnel traffic and status with verify the change is reflected under new visibility field	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.23	Create Gre Tunnel and Enable the tracker and check it should be reflected in Visibility field	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.24	Bring down GRE Tunnel and tracker enabled, Monitor the Security and check Tracker is up & tunnel is Down	Passed	
ENJ.SIGTM.20.10.1_17.10.1_N.25	Configure latency due to tracker down and monitor Event or check through CLI	Passed	

ISE Integration

ENJ.IDF.20.10.1_17.10.1_N01	To integrate ISE with SDWAN Vmanage and AD	Passed	
ENJ.IDF.20.10.1_17.10.1_N02	To Evaluate configured User in the ISE are being reflected in the Vmanage	Passed	
ENJ.IDF.20.10.1_17.10.1_N03	To Evaluate configured User groups in the ISE are being reflected in the Manage	Passed	
ENJ.IDF.20.10.1_17.10.1_N04	To add/delete the user/user group in vmanage and to verify if the same has been updated in ISE and AD	Passed	
ENJ.IDF.20.10.1_17.10.1_N05	To edit the user/user groups in vmanage and to verify if the same has been updated in ISE and AD	Passed	
ENJ.IDF.20.10.1_17.10.1_N06	To check the re-sync performance after terminating the session from vmanage and ISE	Passed	
ENJ.IDF.20.10.1_17.10.1_N07	To Check for the Logs and Reports in the Vmanage for the configured user and user group	Passed	
ENJ.IDF.20.10.1_17.10.1_N08	To Create a set of 18 user in a Group A identity list Cisco ISE and observe the Results	Passed	
ENJ.IDF.20.10.1_17.10.1_N09	To Create a set of 4 user in a Group B identity list Cisco ISE and observe the Results	Passed	
ENJ.IDF.20.10.1_17.10.1_N10	To Restrict the access to YouTube applications for Group B users using ISE integrations	Passed	

ENJ.IDF.20.10.1_17.10.1_N11	To Configure and verify the Identity Group " Employee", "Guest", "Partners", Allowing access to youtube.com only	Passed	
ENJ.IDF.20.10.1_17.10.1_N12	Allowing a Specific user in the Guest to access the Youtube.com and verify the results	Passed	
ENJ.IDF.20.10.1_17.10.1_N13	To configure and verify the URL's visited by Guest user in the Org using ISE integrations	Passed	
ENJ.IDF.20.10.1_17.10.1_N14	To Configure and verify the URL filtering for Identity group "Partners" and allow the access Youtube.com with inspect	Passed	
ENJ.IDF.20.10.1_17.10.1_N15	To Check the user logon session in the vsmart	Passed	
ENJ.IDF.20.10.1_17.10.1_N16	To Check the user logon session in the cat8k platform via OMP	Passed	
ENJ.IDF.20.10.1_17.10.1_N17	Configure Cisco vSmart Controller to Connect to Cisco ISE Using a CLI Template	Passed	
ENJ.IDF.20.10.1_17.10.1_N18	To Configure Cisco SD-WAN Identity-Based Firewall Policy Using a CLI Template	Passed	
ENJ.IDF.20.10.1_17.10.1_N19	To Configure Cisco SD-WAN Identity-Based Firewall Policy Using a CLI Template	Passed	
ENJ.IDF.20.10.1_17.10.1_N20	To Create ZBFW policy for user from the created user group in AD/ISE "Employees" to access Google.com	Passed	

ENJ.IDF.20.10.1_17.10.1_N21	To Create ZBFW policy for user from the created user group in AD/ISE "Employees" to access Yahoo.in Along with inspect	Passed	
ENJ.IDF.20.10.1_17.10.1_N22	To Create ZBFW policy for user from the created user group in AD/ISE "Guest" to Drop the packets routed to Yahoo.in	Passed	
ENJ.IDF.20.10.1_17.10.1_N23	To Create ZBFW policy for user from the created user group in AD/ISE "Guest" to Drop the packets routed to Yahoo.in	Passed	
ENJ.IDF.20.10.1_17.10.1_N24	To Create ZBFW policy for user from the created user group in AD/ISE "Employees" to access Yahoo.in Along with inspect in ASR platform	Passed	
ENJ.IDF.20.10.1_17.10.1_N25	To Restrict the access to User group "Employee “for the Internal Server hosted in DC identical list and verify the results with ACL	Passed	
ENJ.IDF.20.10.1_17.10.1_N26	To Delete the ISE connections and check the user group and user details	Passed	
ENJ.IDF.20.10.1_17.10.1_N27	Verify the behaviour when vSmart reboots	Passed	
ENJ.IDF.20.10.1_17.10.1_N28	Verify the behaviour when "clear omp all" is triggered on vSmart	Passed	
ENJ.IDF.20.10.1_17.10.1_N29	Edit the IP address for existing ISE connection with vManage	Passed	
ENJ.IDF.20.10.1_17.10.1_N30	Edit the username/password for existing ISE connection with vManage	Passed	

ENJ.IDF.20.10.1_17.10.1_N31	To Check for ISE registeration and mapping redistribution when vSmarts are in cluster	Passed	
ENJ.IDF.20.10.1_17.10.1_N32	Edit the username/password for existing ISE connection with vManage	Passed	

SDWAN UX 2-0 - Configuration 2-0-Feature Profiles and Configuration Groups

Logical ID	Title	Status	Defect ID
ENJ.CFP.20.10.1_17.10.1.N.01	To create a configuration group workflow for a single router	Passed	
ENJ.CFP.20.10.1_17.10.1.N.02	To Use the new simplified workflow introduced in 20.9 to create configuration group	Passed	
ENJ.CFP.20.10.1_17.10.1.N.03	To resume the Configuration Group Workflow	Passed	
ENJ.CFP.20.10.1_17.10.1.N.04	To add Devices to a Configuration Group Using Rules and operations	Passed	
ENJ.CFP.20.10.1_17.10.1.N.05	To Create management VPN feature	Passed	
ENJ.CFP.20.10.1_17.10.1.N.06	To switch the profile to another profile	Passed	
ENJ.CFP.20.10.1_17.10.1.N.07	To add feature and sub feature to perform LAN routing	Passed	
ENJ. CFPCG.20.10.1_17.10.1. N.08	To create SVI profile using routing option with enabling the track OMP	Passed	
ENJ.CFP.20.10.1_17.10.1.N.09	To edit SVI profile	Passed	
ENJ.CFP.20.10.1_17.10.1.N.10	To create ThousandEyes profile with version v2/V	Passed	
ENJ.CFP.20.10.1_17.10.1.N.11	To Add/Remove/deploy associated devices from config groups	Passed	
ENJ.CFP.20.10.1_17.10.1.N.12	To Create Thousand Eye Parcel via API	Passed	
ENJ.CFP.20.10.1_17.10.1.N.13	To Get SNMP details of an SNMP parcel via API	Passed	
ENJ.CFP.20.10.1_17.10.1.N.14	To Associate WAN BGP to Transport VPN via API	Passed	

ENJ.CFP.20.10.1_17.10.1.N.15	To Change System ID via Global Parcel API	Passed	
ENJ.CFP.20.10.1_17.10.1.N.16	To disassociate the profile	Passed	
ENJ.CFP.20.10.1_17.10.1.N.17	To create Global parcel using global settings and other settings	Passed	
ENJ.CFP.20.10.1_17.10.1.N.18	To delete Global parcel	Passed	
ENJ.CFP.20.10.1_17.10.1.N.19	To create a cellular interface under configuration group feature with associated Tunnel and NAT	Passed	
ENJ. CFPCG.20.10.1_17.10.1. N.20	To create tracker to the WAN parcel	Passed	
ENJ.CFP.20.10.1_17.10.1.N.21	To Configure user and authentication with SNMP version 3	Passed	
ENJ.CFP.20.10.1_17.10.1.N.22	To trap the target server with SNMP V3	Passed	
ENJ.CFP.20.10.1_17.10.1.N.23	To create SNMP V3 parcel with view and community	Passed	
ENJ.CFP.20.10.1_17.10.1.N.24	To change the authentication of user using SNMP V3 parcel	Passed	
ENJ.CFP.20.10.1_17.10.1.N.25	To associate WAN VPN to WAN BGP parcel	Passed	
ENJ.CFP.20.10.1_17.10.1.N.26	To create BFD parcel	Passed	
ENJ.CFP.20.10.1_17.10.1.N.27	To edit LAN VPN Parcel	Passed	
ENJ.CFP.20.10.1_17.10.1.N.28	To create a Localized policy using cli profile	Passed	
ENJ.CFP.20.10.1_17.10.1.N.29	To Create system profile via API	Passed	
ENJ.CFP.20.10.1_17.10.1.N.30	To add tags to devices using vmanage	Passed	

PPP Dialer interface support for DIA NAT use-cases

Logical ID	Title	Status	Defect ID
ENJ.PPP.20.10.1_17.10.1_N.01	Configure the Dialler interface with Ip address and Dialler pool over PPP	Passed	
ENJ.PPP.20.10.1_17.10.1_N.02	Configure to enable the PPPOE with Dialler pool by using physical interface	Passed	
ENJ.PPP.20.10.1_17.10.1_N.03	Configure the DIA for NAT fallback with Dialler interface by using Secondary interface	Passed	
ENJ.PPP.20.10.1_17.10.1_N.04	Configure the Dialler interface support for DIA NAT by using loopback interface	Passed	
ENJ.PPP.20.10.1_17.10.1_N.05	Configure the static ip address negotiated support for Dailer with NAT DIA	Passed	
ENJ.PPP.20.10.1_17.10.1_N.06	Configure the Dailer interface for DIA in PPPOE by CHAP in PPP encapsulation	Passed	
ENJ.PPP.20.10.1_17.10.1_N.07	Configure the Dailer interface for DIA in PPPOE by CHAP in PPP encapsulation	Passed	
ENJ.PPP.20.10.1_17.10.1_N.08	Configure the ip Nat inside through Vmanage by enabling the NAT type with interface	Passed	
ENJ.PPP.20.10.1_17.10.1_N.09	Configure the PPPOE Dailer by using sub interface	Passed	
ENJ.PPP.20.10.1_17.10.1_N.10	Configure the PPP Dailer interface to track the dual endpoint tracker by using WAN Interface	Passed	

ENJ.PPP.20.10.1_17.10.1_N.11	Configure the PPP interface with enable the PPPOE over encapsulation PPP	Passed	
ENJ.PPP.20.10.1_17.10.1_N.12	configure the PPPoE Dailer interface to track the endpoint IP addresS	Passed	
ENJ.PPP.20.10.1_17.10.1_N.13	Configure the PPPOE in Dailer interface with TCP MSS and NAT DIA	Passed	
ENJ.PPP.20.10.1_17.10.1_N.14	Configure the Dailer interface support for NAT DIA with endpoint tracker Along with PPPOE	Passed	
ENJ.PPP.20.10.1_17.10.1_N.15	Configure the PPP dialler interface to track the DNS server with type of interface	Passed	
ENJ.PPP.20.10.1_17.10.1_N.16	To configure Dailer interface with ip nat outside with encapsulation ppp	Passed	
ENJ.PPP.20.10.1_17.10.1_N.17	Configure the PPPOE over Sub interface PPP by using CLI	Passed	
ENJ.PPP.20.10.1_17.10.1_N.18	PPPoE Dialer with NAT interface overload by using Vmanage	Passed	
ENJ.PPP.20.10.1_17.10.1_N.19	Configure the PPPOE Dialer with Encapsulation PPP by Using Vmanage	Passed	
ENJ.PPP.20.10.1_17.10.1_N.20	Configure the PPPOE Dailer with NAT and endpoint tracker by using Vmanage	Passed	
ENJ.PPP.20.10.1_17.10.1_N.21	Configure the Dialler with NAT DIA interface overload using Static inside	Passed	
ENJ.PPP.20.10.1_17.10.1_N.22	Configure PPPOE Dialler interface with static port forwarding by using HTTP	Passed	

ENJ.PPP.20.10.1_17.10.1_N.23	Configure PPPOE Dailer egress interface with port forwarding by using Telnet	Passed	
ENJ.PPP.20.10.1_17.10.1_N.24	Configure the PPPOE with NAT DIA interface pool overload	Passed	
ENJ.PPP.20.10.1_17.10.1_N.25	Configure and Check whether PPPOE NAT Translation exists if the device as reloaded	Passed	

App aware routing for IPv6

Logical ID	Title	Status	Defect ID
ENJAARIPV620.10.1_17.10.1_N.01	To Configure the AAR policy for ipv6 using vmanage	Passed	
ENJAARIPV620.10.1_17.10.1_N.02	To Configure the AAR policy with dual stack using vmanage	Passed	
ENJAARIPV620.10.1_17.10.1_N.03	To Configure the Best Tunnel path for IPV6 using backup-preferred colour	Passed	
ENJAARIPV620.10.1_17.10.1_N.04	To Configure the Best Tunnel path for IPV6 using Fallback-to-best-path	Passed	
ENJAARIPV620.10.1_17.10.1_N.05	To Configure the Best Tunnel path for Dual stack using backup-preferred colour	Passed	
ENJAARIPV620.10.1_17.10.1_N.06	Configure BFD parameters Hello Interval 1000ms and poll interval 30s & multiplier 2 and observe the performance for AAR for IPv6	Passed	
ENJAARIPV620.10.1_17.10.1_N.07	Configure the Application Aware Routing for IPv6 using CLI	Passed	
ENJAARIPV620.10.1_17.10.1_N.08	To Configure and verify the AAR policy for ipv6 using vmanage in ISR platform	Passed	
ENJAARIPV620.10.1_17.10.1_N.09	To Configure the Best Tunnel path for IPV6 using backup-preferred color in ISR platform	Passed	

ENJ.AARIPV6.20.10.1_17.10.1_N.10	To Configure the Best Tunnel path for IPV6 using Fallback-to-best-path in ISR platform	Passed	
ENJ.AARIPV6.20.10.1_17.10.1_N.11	To Configure and verify the AAR policy using Default action for IPv6	Passed	
ENJ.AARIPV6.20.10.1_17.10.1_N.12	To Configure and Verify the AAR Policy based on Strict SLA Class for IPv6	Passed	
ENJ.AARIPV6.20.10.1_17.10.1_N.13	To Configure and Verify the AAR Policy based on Strict SLA Class for Dual Stack	Passed	
ENJ.AARIPV6.20.10.1_17.10.1_N.14	To Configure and verify the AAR apply policy to specific Site and VPN.00	Passed	
ENJ.AARIPV6.20.10.1_17.10.1_N.15	To Monitor the Data plane Tunnel Performance for AAR ipv6	Passed	
ENJ.AARIPV6.20.10.1_17.10.1_N.16	To Configure and Verify the AAR Policy based on Strict SLA Class for IPv6 with ASR platform	Passed	

Related Documents

Related Documentation

Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release 17.10 Release Notes

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/17-10/sd-wan-rel-notes-xe-17-10.html

Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.10

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 17.10

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 17.10

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

Cisco SD-WAN Monitor and Maintain Configuration Guide,Cisco IOS XE Release 17.10

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/m-applications-performance-and-site-monitor.html

Cisco SD-WAN Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.10

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

Cisco SD-WAN Security Configuration Guide, Cisco IOS XE Release 17.10

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/intrusion-prevention.html#update-ips-signatures-from-release-17-10