CITRIX SD-WAN 11.1.0 Release Notes

Version 1

Copyright and Trademark Notice

Contents

Introduction

This release note describes what's new, fixed issues, and known issues applicable to Citrix SD-WAN software release 11.1.0 for the SD-WAN Standard Edition, WAN Optimization, Premium Edition appliances, and SD-WAN Center.

For information about the previous release versions, see the Citrix SD-WAN documentation.

What's New

Application-centric enhancements

Zero Touch enhancements

Citrix SD-WAN now supports Zero Touch Provisioning on certain designated data ports on the SD-WAN 110 Standard Edition (SE) and SD-WAN VPX platforms. Zero Touch Deployment (ZTD) is now supported on the designated data ports and there is no need to use a separate management port for ZTD.

[NSSDW-20641]

Default and fall-back configuration

The Citrix SD-WAN 110 SE, 210 SE, 410 SE, 1100 SE/PE, VPX, and VPX-L platforms are shipped with a default configuration to provide basic in-band management after a configuration reset. The default configuration can be modified by the user and, if enabled, is used as a fall-back configuration in the event of a critical failure.

[NSSDW-20641]

In-band management enhancements

Citrix SD-WAN now supports SNMP and SD-WAN Center connectivity through in-band management interfaces. This means that separate connectivity via the designated management port is no longer required to connect SD-WAN appliances to Citrix SD-WAN Orchestrator or SD-WAN Center. Management IP reporting for SD-WAN Center connectivity requires an in-band Virtual IP address to be configured as the backup management network.

[NSSDW-24533]

Microsoft Office 365 beacon service

Citrix SD-WAN supports Microsoft Office 365 beacon probing capability to help determine the best link to be used for Office 365. The probes determine the latency (round-trip-time) involved in reaching Office 365 endpoints through each WAN link, enabling network administrators to identify the best link to be used for O365 traffic. The Office 365 beacon probing capability is configured only through Citrix SD-WAN Orchestrator.

[NSSDW-14231]

IPv6 support

Citrix SD-WAN provides the following IPv6 capabilities:

- Configuration infrastructure for IPv6 WAN links.
- Establishment of Virtual Path Tunnels over IPv6 networks.

From 11.1.0 release onwards, two subsections are available under **Virtual IP Address**: IPv4 and IPv6 addresses. The IPv6 addresses are used to support untrusted interfaces. The untrusted interfaces can be used to tunnel routable IPv4 traffic over IPv4 or IPv6 virtual paths.

[NSSDW-1913, NSSDW-1929, NSSDW-1936]

ICA session reconnect

Citrix SD-WAN supports ICA session reconnects with HDX Insight NSAP virtual channel. If you lose the connection, the connection reconnects without re-entering the login credentials. The default value is 180 seconds. It can be configured through VDA's policy.

[NSSDW-15457]

Routing enhancements

Static Inter-routing domain service

Citrix SD-WAN now provides **Static Inter-routing Domain** service, enabling routing between Routing Domains within a site or between different sites. This eliminates the need for an external edge router to handle routing between two routing domains. The inter-routing service can further be used to set up routes, firewall policies, and NAT rules.

[NSSDW-1966]

GRE tunnel support on intranet service

Citrix SD-WAN enables configuring GRE tunnels in active/passive mode over single or multiple WAN links. An intranet service must be created for each GRE tunnel.

[NSSDW-16112]

Cloud services

Cloud Direct Billing Mode option

The Cloud Direct **Billing Mode** option is introduced in Citrix SD-WAN Center. This enables the use of Cloud Direct trial/evaluation licenses, which can be provided by Citrix sales or authorized partners. Sites operating with Cloud Direct evaluation licenses should be set to the **Demo** Billing Mode option. Sites upgrading to full Cloud Direct subscription licenses should be set to the **Production** Billing Mode option.

[NSSDW-21047]

Azure Virtual WAN

Azure Virtual WAN – Hub-to-Hub communication

Azure Virtual WAN customers can now leverage Microsoft's global backbone network for inter-region hub-to-hub communication (Global transit network architecture). This enables branch to Azure, branch-to-branch over Azure backbone, and branch to hub (in all Azure regions) communication.

You can leverage Azure's backbone for inter-region communication only when you purchase the Standard SKU for Azure Virtual WAN. For pricing details, see Virtual WAN pricing. With the Basic SKU, you cannot use Azure's backbone for inter-region hub-to-hub communication. For more details, see Global transit network architecture and Virtual WAN.

[NSSDW-14171]

Multiple WAN link support for Microsoft Virtual WAN connectivity

Citrix SD-WAN supports multiple WAN links in primary and secondary fashion to establish an IPsec tunnel towards Azure Hubs. This provides link level redundancy at the site. If the primary link fails, the configured tunnel towards Azure Hub is re-established using the secondary WAN link. On WAN link failure, the tunnel is re-established after the DPD timer expires. The default time is 300 seconds.

[NSSDW-22161]

Dual WAN link support for IPsec connectivity

Citrix SD-WAN enables the use of two WAN links for establishing IPsec tunnels to guard branch environments against periods of service disruption. If the primary tunnel goes down for any reason, the secondary tunnel becomes active. This is also available for Azure virtual WAN.

[NSSDW-17871]

Deployments

Citrix SD-WAN SE on OpenStack using CloudInit

Citrix SD-WAN SE can now be deployed in an OpenStack environment. For this, Citrix SD-WAN image must support config-drive functionality. CloudInit script supports contextualization for SD-WAN deployment in OpenStack with config-drive.

For SD-WAN instance in OpenStack, the inputs needed are Management IP, DNS, and serial number. The CloudInit script parses these inputs and provision the instance with the given information.

[NSSDW-20638]

Citrix SD-WAN VPX SE on ESXi 6.5

Citrix SD-WAN SE VPX software is now available as a VMware vSphere virtual machine running under ESXi 6.5.

[NSSDW-20306]

Establish IPsec tunnels on DHCP enabled interfaces using dynamic IPs

Citrix SD-WAN can now establish IPsec tunnels when a WAN link directly terminates on the appliance and a dynamic IP is assigned to the WAN link.

Intranet IPsec tunnels must be configurable when the local tunnel IP address is not or cannot be known. The label for an unset address is changed to <**Auto**> when the tunnel type is **Intranet**. If the **Local IP** is set as <**Auto**>, it takes the IP address that is incorporated for the access interface on that WAN link. The WAN link access interface might get the IP address either statically or from DHCP.

[NSSDW-17869]

Security enhancements

PKI enhancement – certificate distribution

Citrix SD-WAN supports appliance authentication for static and dynamic virtual paths using Public Key Infrastructure (PKI) as an additional security feature. Enabling the feature extends the existing virtual path authentication mechanism by distributing PKI certificates over the data path, by the appliance initiating the exchange. The PKI enhancement also supports Certificate Revocation List (CRL) management for centralized revocation of compromised certificates.

[NSSDW-21622]

UI enhancements

Site name in SD-WAN GUI banner

The site name is displayed on the SD-WAN appliance GUI header.

[SDWANHELP-921]

Multi-user access warning

When a user logs in into a Citrix SD-WAN appliance, a warning message displays the user name of other users who are currently logged into the appliance.

[NSSDW-23279]

Platforms

Citrix SD-WAN 110 SE

The Citrix SD-WAN 110 SE platform is a new branch side appliance that can be deployed in micro and small branch offices/ remote sites/ retail stores, homes, and temporary worksites. A single box-in-branch solution helps to reduce the hardware footprint and eases branch deployment.

The Citrix SD-WAN 110-SE appliance is a desktop form factor appliance.

The new device comes in two models:

- SD-WAN 110
- SD-WAN 110-LTE-WiFi

Note: Release 11.1.0 on the SD-WAN 110-LTE-WiFi model does not support Wi-Fi capabilities. This capability will be enabled in a future release.

[NSSDW-2010]

Citrix SD-WAN 6100 SE performance improvements

Citrix SD-WAN 6100 SE appliance virtual path limit is increased from 550 to 1,000 static virtual paths.

[NSSDW-1919]

Citrix SD-WAN 210 SE and 210 LTE license support

Citrix SD-WAN 210-SE and 210-LTE appliances now support a 300 Mbps license option.

[NSSDW-20458]

PAN-OS 8.1.x support for VM-series hosted on Citrix SD-WAN 1100 appliance

Citrix SD-WAN 1100 appliances now support PAN-OS 8.1.3 in addition to 9.0.1 for Palo Alto VM-Series.

[NSSDW-23396]

System enhancements

License server update

The license server is updated to version 11.16.3.

[NSSDW-20534]

Improved logging format

The new SD-WAN logs format displays the time of the day at which the logs were captured instead of the last known uptime.

[NSSDW-23297]

Fixed Issues

SDWANHELP-1206: A code bug leading to unnecessary restart of SNMP daemon when main configuration update is done. This was causing a false appliance reboot trap. The issue is applicable only to SD-WAN 110, SD-WAN 210, SD-WAN 410, SD-WAN 1100, and SD-WAN VPX platforms.

SDWANHELP-1203: The SD-WAN appliances crashes multiple times after upgrading to version 11.0.3 from version 10.2.3. The crash happens when a branch, configured as an intermediate site between two remote sites, cannot handle the traffic beyond the threshold.

The branch tries to form a dynamic virtual path between the two sites, while the remote sites are connected to it through the dynamic virtual path instead of the static virtual path. The fix ensures that the branch will not act as an intermediate site for two remote sites when it is connected to any of them via a dynamic virtual path.

SDWANHELP-1193: When the MCN is in the factory state while downloading the LCM package without activating the staged software/configuration, the LCM package downloaded is about the same size as the configurations (hundreds of KB).

This issue occurs when you perform Change Management on a factory state MCN. Try to download the LCM package immediately after clicking **Staging** (when the download link is available), but before clicking **Activating Staged**.

SDWANHELP-1187: Users unable to change LOM user password.
CLI support to configure IP and password for the LOM port is introduced on the following appliances, running 11.1.0 and newer versions.

- 6100 SE
- 5100 SE
- 4100 SE
- 2100 SE
- 5100 PE
- 2100 PE

Supported commands are as follows:

status # Show status
disable # Disable LOM access
enable dhcp # Enable DHCP address on LOM
enable static <ip> <mask> <gateway> # Enable static IP address on LOM
password # Change LOM password

SDWANHELP-1180: Citrix SD-WAN MCN UI is unresponsive when a new site is added and the configuration is pushed. The MCN event logs have **SQL error: ERROR - mysqld not available** log for a long time.

SDWANHELP-1179: NITRO API to get flows statistics was returning **LAN to WAN** as flow direction for all flows irrespective of the correct direction. This issue was observed only with NITRO API and not on the GUI.

SDWANHELP-1164: On transferring the appliance settings from SD-WAN Center, if the password, in the appliance settings, contains dollar symbol followed by some character, then the transfer fails. For example, the passwords test$1, test$1$d will fail. But test1$ will work.

SDWANHELP-1160: The Citrix SD-WAN Center displays duplicate IP addresses under WAN links for a site in the Configuration Editor. The issue occurs when the fourth number in any two WAN link IP addresses starts with the same digit and varies by the number of digits like 4, 45, 486 and so on.

SDWANHELP-1122: The host name of a Citrix SD-WAN WANOP instance can be changed from the GUI and the changed host name is reflected after reboot. On some Citrix SD-WAN WANOP instances, which serve as an arbitrator, the host name is not persistent across reboots.

NSSDW-23485: Cloud Direct does not allow to perform any operation if the active configuration on the MCN has a dot character in its name. The configuration file name had to be updated to not include dot character.

SDWANHELP-1115 - If the MPLS queue rate unit is set to %, LAN to WAN and WAN to LAN permitted rates shows 0 on **Provisioning groups** and **Provisioning services** screen. After the fix the provisioning section displays value in kbps after converting the % values internally.

If MPLS queue rate unit is set to %, LAN to WAN and WAN to LAN permitted rates shows 0 on **Provisioning groups** and **Provisioning services** screen.

SDWANHELP-1110: In a rare scenario, a data path crash might happen when dynamic virtual paths are used.

SDWANHELP-1097: At times, while running ICA traffic, the appliance reboots. The issue might happen if the ICA VDA or client sends ICA packets with a format that is not expected by SD-WAN.

NSSDW-21806: On configuring PPOE settings - AC Name, Service Name, and Username in uppercase, the entries get converted to lower case which can cause problem in IP learning from the Access Concentrator (ISP).

SDWANHELP-1016: When a WAN link is changed from **Private MPLS** to **Private Intranet/Internet**, the configuration editor shows EC159, EC160, EC178, EC179 audit errors. Post this fix, the user has to navigate to **Configuration Editor** > **Connections** > **WAN Links** > **Virtual Path link** and enable **Use** option to use **Private Intranet/Internet** type and avoid further audit errors.

SDWANHELP-959: Citrix SD-WAN appliance is rebooted due to a crash in route look-up. The issue might occur when the traffic between two branches is below the dynamic virtual path threshold, leading to dynamic virtual path expiry.

NSSDW-19132: In case of HDX MSI Sessions, connection state is shown as **INVALID** for some of the IDLE streams in the **HDX User Sessions** report under HDX tab of SDWAN Center reporting. The fix is to show the connection state as **INACTIVE** for idle streams of MSI sessions.

SDWANHELP-760: In a rare scenario, a possible race condition with route update engine when dynamic routing is used leading to a crash.

SDWANHELP-943: Creation of the bridge pair was possible on all interfaces and hence auditing the configuration would clear the bridge pair on non-fail-to-wire ports. Now bridge pairs can be created only on interfaces that support fail-to-wire.

SDWANHELP-738 : The Citrix SD-WAN service crashes periodically. The crash happens randomly on some SD-WAN 210 LTE boxes. The fix is to upgrade the LTE modem firmware to the latest SD-WAN software version, or perform a single step software upgrade to SD-WAN version 10.2.6 or newer.

NSSDW-24559: Incorrect route table values are seen in SNMP query for the route table. The CITRIX-SDWAN-MIB file is modified, upload the new CITRIX-SDWAN-MIB file in the SNMP manager to fix this issue.

SDWANHELP-1174: In a few cases, NetFlow/IPFIX collector (for example - SolarWinds) bandwidth report aggregates bandwidth usage over multiple sample intervals. This issue results in incorrect plotting of bandwidth usage graphs. Although the **Total Bandwidth** per flow is reported correctly.

SDWANHELP-1191: In a few cases, NetFlow/IPFIX collectors (for example - SolarWinds) will report spikes in bandwidth usage due to a corner case code issue.

NSSDW-25135: At times, during Zscaler deployment, wrong configurations were used to create the mapping. The issue occurs due to erroneous duplicate entries in the database. The fix ensures that there are no duplicate entries in the database.

NSSDW-23795: In few cases, NetFlow/IPFIX collectors (for example, SolarWinds) reporting results in MYSQL error = (1064) in SDWAN_firewall.log. This issue results into incorrect plotting of bandwidth usage graphs.

NSSDW-24862: Citrix SD-WAN is not sending the NetFlow data to the collectors at regular interval.

Known Issues

NSSDW-21808: The provisioned appliance information on SD-WAN Center gets cleared before the actual de-provision operation gets completed on the appliance. If any error occurred during de-provisioning, then the user will not be able to perform any Palo Alto specific operations on the appliance from the SD-WAN Center.

Workaround: Select the missing site and click **Provision** to restore the appliance information.

NSSDW-24895: The SD-WAN Center upgrade from version 10.2.6 or lower to version 11.1.0 fails. Uploading package fails with the error - **Invalid file Name**.

Workaround: To upgrade SD-WAN Center from version 10.2.6 or lower to version 11.1.0, first upgrade to version 11.0.3 and then upgrade to version 11.1.0.

NSSDW-25313: In Citrix SD-WAN Center, the MCN discovery fails after adding secondary storage.

Workaround: Regenerate the Citrix SD-WAN Center certificate and upload it to the MCN.