

Dell SmartFabric OS10 10.5.4.10 Release Notes

This document describes the new and changed features, restrictions, resolved issues, and known issues in the Dell SmartFabric OS10 Release 10.5.4.10.


Current Release Version: 10.5.4.10

Release Date: 2024-10-25

Previous Release Version: 10.5.4.8 (PowerSwitch) and 10.5.4.9 (PowerEdge MX)

The information in this document is applicable to all the switches listed in the [Supported hardware](#) section.

For documentation about the Dell open network install environment (ONIE)-enabled hardware switches, see [Dell Networking](#).

 **NOTE:** This release is intended for both PowerSwitch and PowerEdge MX users.

Document revision history

Table 1. Revision History

Revision	Date	Description
A01	2024-10-25	The N3224F-ON platform has been removed from the Supported platforms section. Updated the 1G auto negotiation details to the Known software behavior -OS10 section.
A00	2023-09-21	10.5.4.10 Release—Added new features to the New and changed in 10.5.4.10 section. Added AR-43237, AR-43001, AR-42921, AR-43043, AR-42979, AR-43063, AR-43027, AR-43232, AR-42975, AR-43116, AR-43011, AR-42490, AR-42161, and AR-43137 to the Resolved issues in 10.5.4.10 section. Added AR-43224, AR-43074, AR-43230, AR-41049, AR-42284, and AR-43037 to the Known issues in 10.5.4.10 section.

Supported hardware

The current release is supported on the following:

- Dell PowerSwitches
 - S3048-ON
 - S4048-ON, S4048T-ON
 - S4112F-ON, S4112T-ON
 - S4128F-ON, S4128T-ON
 - S4148F-ON, S4148FE-ON, S4148T-ON, S4148U-ON
 - S5232F-ON, S5248F-ON, S5296F-ON
 - S5212F-ON, S5224F-ON
 - S5448F-ON
 - S6010-ON
 - Z9100-ON
 - Z9264F-ON
 - Z9332F-ON
 - N3248TE-ON
 - Z9432F-ON (In SFS deployments, this switch can only be used as a spine switch.)
 - E3224F-ON
 - Z9664F-ON
- Dell PowerEdge MX7000 with the following Ethernet modules:
 - MX9116n Fabric Switching Engine
 - MX5108n Ethernet Switch



Related documentation

This section lists the documentation that is related to 10.5.4.10.

- [Dell SmartFabric OS10 User Guide](#)
- [Dell SmartFabric OS10 Installation, Upgrade, and Downgrade Guide](#)


See [Dell SmartFabric OS10 Documentation page](#) to download these documents.

New and changed in 10.5.4.10

Table 2. New and changed features

Functional Area	Feature Description	Summary of Benefits
Security	Linux Kernel upgrade	The Linux kernel version has been upgraded from 4.19.249 to 4.19.269-1.
Security	The following Dell Security Advisory has been addressed: <ul style="list-style-type: none">• DSA-2023-278	This product release contains security updates. Once available, information will be accessible on the Dell Security Advisories, Notices, and Resources website.

Known Software Behavior - OS10

 **NOTE:** The software behaviors that are mentioned here are applicable to OS10.5.4.10.

Flow control configuration

- If a flow control change is performed on an autonegotiation-enabled port, the port flaps once for the change to take effect.
- If a DAC (25G/40G/50G/100G/200G/400G) is connected to a switch, autonegotiation is enabled by default.


1G auto negotiation

All Dell PowerSwitches:

Platforms (Z9100, Z9264F, Z9332F-ON, Z9432F-ON, S5200 Series, S5448F-ON, S4100 Series, and S4200 Series with 25G (SFP28), 100G (SFP56DD, QSFP28), 200G (QSFP28DD), and 400G (QSFP56DD) ports do not support 1G auto negotiation.

OS10 upgrades

- When upgrading from 10.5.0 to 10.5.2 or later, the upgrade goes through the ONIE install process and displays an ONIE update log. This does not indicate an upgrade failure. Do not interrupt the upgrade process as it proceeds automatically.
- Upgrading OS10 nodes in SmartFabric mode from Release 10.5.3.1 or earlier to Release 10.5.3.2 or later:

 **NOTE:** The following procedure is not applicable if the OS10 switch is already running Release 10.5.3.2 or later software, or if the switch is in Full Switch mode. Use the `show switch-operating-mode` command to check the switch mode.

Before you upgrade the fabric, you must run the following `curl` command on each of the leaf nodes in the deployment. Run this command on the leaf nodes one after another continuously. You can run this command in any one of the following ways:

- Run this command from a remote server using the leaf node's management IP address if the node is reachable:

```
login-chn-02:/swt_scripts_repo/feature/SFS> curl -i -k -H "Accept: application/json" -H "Content-Type: application/json" -u REST_USER:admin -d '{"nvo-evpn:evpn":{"disable-rt-asn":true}}' -X PATCH https://10.10.72.184/restconf/data/nvo-evpn:evpn
```


```
HTTP/1.1 204 No Content
Server: nginx
Date: Thu, 04 Aug 2022 06:44:47 GMT
Connection: keep-alive
Cache-Control: no-cache
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-XSS-Protection: 1; mode=block
login-chn-02:/swt_scripts_repo/feature/SFS>
```

Where 10.10.72.184 is the management IP address of the leaf node.


- o If you have not configured a management IP address or if the node is not reachable, log in to the leaf node through the console and enter the following command using the loopback address:

```
LEAF1# system "sudo -i"
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
#1) Respect the privacy of others. #2) Think before you type. #3) With
great power comes great responsibility.
[sudo] password for admin:
root@POD3-LEAF1:~#
root@POD3-LEAF1:~# curl -i -k -H "Accept: application/json" -H "Content-Type: application/json" -u
REST_USER:admin -d '{"nvo-evpn:evpn":{"disable-rt-asn":true}}' -X PATCH https://127.0.0.1/restconf/
data/nvo-evpn:evpn
HTTP/1.1 204 No Content
Server: nginx
Date: Thu, 04 Aug 2022 06:40:15 GMT
Connection: keep-alive
Cache-Control: no-cache
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-XSS-Protection: 1; mode=block
LEAF1:~#
```

- o You can also use any API tool such as Postman on the leaf nodes.

 **NOTE:** Without running the `curl` command on the leaf nodes, if you upgrade from Release 10.5.3.1 or earlier to Release 10.5.3.2 or later, traffic loss for about 5 to 7 minutes is observed.

Known Software Behavior - Dell PowerEdge MX


 **NOTE:** The software behaviors that are mentioned here are applicable to OS10 revision 10.5.0.1 and later.

Ethernet Modules

- When upgrading from earlier releases to 10.5.0.7, aaa authentication configuration with nonlocal authentication methods as the first target in the startup configuration gets rejected and replaced with the default aaa authentication configuration: `aaa authentication login default local`.
- If you configure multiple authentication methods on Dell PowerEdge MX7000 Ethernet modules - MX9116n Fabric Switching Engine and MX5108n Ethernet Switch, you must configure local authentication as one of the methods in the list. Before 10.5.1.6, `local` authentication had to be the first method in the list.
- From 10.5.1.6, if you configure multiple authentication methods on Dell PowerEdge MX7000 Ethernet modules - MX9116n Fabric Switching Engine and MX5108n Ethernet Switch - you must configure local authentication as one of the methods in the list.


False Errors on FC Ports

- The `total errors` count in the `show interface fibrechannel` command output displays incorrect values during FC port flaps, IOM reboot, or port conversion from ETH to FC, followed by bringing up of the FC port.


 **NOTE:** This behavior is applicable only to the MX9116n.

Fibre Channel

- After you change the FC Map on FIP snooping enabled active VLAN sessions, use the `shut` and `no shut` commands to reestablish the FCoE sessions.
- The maximum number of members in an FC Zone is 255.

 **NOTE:** This behavior is applicable only to the MX9116n.

- For the `default-zone` settings to work properly, ensure that the maximum number of logged-in FC and FCoE nodes is less than 120.

 **NOTE:** This behavior is applicable only to the MX9116n.

- FCoE-generated Access Control Lists (ACLs) take precedence over user-configured ACLs. A user-configured ingress ACL entry cannot deny FCoE and FIP snooping frames.
- After you remove the `vfabric` configuration from an interface, to configure the MTU to default value, configure the nondefault MTU and then configure the default MTU.
- In a FIP snooping bridge, FIP and FCoE frames ingressing on a PFC mismatch interface are dropped.

 **NOTE:** This behavior is only applicable to the MX9116n and MX5108n.

- PFC mismatch on a port channel member port drops FIP and FCoE frames ingressing on that member port, but the learned Enode/Session/FCF information that is associated with the port channel is retained. This results in FCoE show commands displaying misleading information. To resolve this issue, check and correct the PFC configuration on both the ends.
- When you configure a port channel as VLT port channel, the port channel goes down operationally and comes up in the local device. The physical interfaces are operationally up. This leads to the switch removing the FCoE sessions. The remote server is not aware of the port channels being up and down, so the server maintains the FCoE sessions. As these sessions are not available in the switch, the FCoE frames are dropped in the switch. To resolve this, manually flap the port channel.

Login delay

- When logging into a switch, it may take 6 to 10 seconds for the CLI prompt to display.

MTU

- After upgrading to 10.5.1.6 in Full Switch mode, the MTU defaults to 9216 on all VLANs and Ethernet Interfaces which do not already have a user configured MTU.

Obscure password


- Obscure password (`service obscure-password`) is enabled by default when upgrading to 10.5.1.6 if the setting is left untouched before upgrade.
- If obscure password configuration is explicitly disabled before upgrade, it remains in disabled state after upgrade.

Source MAC address handling

- Learning of source MAC address from received LLDP and LACP packets is disabled.

VLAN scale

- If the number of configured VLANs is more than 500, it is recommended to have IGMP/MLD snooping enabled only on the required VLANs and do not exceed a maximum count of 500 enabled VLANs. Alternatively, disable IGMP/MLD snooping globally.

 **NOTE:** IGMP/MLD snooping is disabled by default in MX-Series SFS mode but is enabled in Full Switch mode. See the *Dell SmartFabric OS10 User Guide* for more information.

Known hardware behavior in 10.5.4.10

Fan LED

- On an OS10 S3048-ON switch with reverse airflow:
 - When all fans are operational, the Fan LED is solid amber.
 - When a fan fails, the Fan LED is blinking amber.
- On an OS10 S3048-ON switch with normal airflow:
 - When all fans are operational, the Fan LED is solid green.
 - When a fan fails, the Fan LED is blinking green.

PSU

- If the PSU fan is inactive for more than 15 seconds, the PSU goes into a latched shutdown state and remain in the same state until the AC power cable is removed and reinserted.


Resolved issues in 10.5.4.10

The following high severity issues have been resolved in this release.

Table 3. Resolved issues

Issue ID	Functional Area	Description
AR-43237	AAA Authentication	For a new login session using TACACS authentication over management VRF, the OS10 switch sends the loopback IP as the remote IP address to the TACACS server.
AR-43001	BFD,VLT	In a square VLT setup, when a BFD packet with an unknown destination MAC is received, it is looped continuously.
AR-42921	BGP	When a BGP update message with BGP community attribute is processed, the dn_sm process fails to lead to a system reboot.
AR-43043	BGP	When the device has multiple BGP neighbors, the snmpwalk for BGP peer status misses some of the L2VPN peers.
AR-42979	CLISH	When you run show command with the grep option, unnecessary escape sequence characters are displayed in the output.
AR-43063	DHCP Snooping	When DHCP broadcasts the packet with snooping enabled and without DHCP option 82, it floods all the VLT port channel member ports and VLTi from applications.
AR-43027	Infra:IFM	A crash occurs when changing dynamic lag to static lag with LACP individual configured.
AR-43232	Infra Logging	When you run <code>dcbx version ieee</code> command under the <code>interface range</code> command, a "value is not set" error is displayed.
AR-42975	PAS Media	When you enable the DOM feature for DAC cables, the link flaps because they do not support the DOM feature.

Table 3. Resolved issues (continued)

Issue ID	Functional Area	Description
AR-43116	Radius	In certain scenarios, radius authentication stops working after upgrading OS to 10.5.4.7.
AR-43011	SNMP	When the PSU cable is unplugged or not inserted, the snmpwalk returns "No such instance currently exists at this OID" message instead of Failed and not Present message respectively.
AR-42490	SAI:BCM	Output discards are seen on the interfaces.  NOTE: This issue is only seen on the S4112F-ON switch.
AR-42161	SNMP	When snmpwalk and snmpget commands are run over the nondefault VRFs, it is taking longer time to show the output than usual.
AR-43137	VxLAN	When an untagged vlan is configured, the show virtual-network interface command does not display information about the untagged vlan.

Resolved issues in Previous Releases

The following issues were resolved in earlier 10.5.4 releases.

Table 4. Previous resolved issues



Issue ID	Resolved in	Description
AR-43001	10.5.4.9	In a square VLT setup, when a BFD packet with an unknown destination MAC address is received, it is looped continuously.
AR-43138	10.5.4.9	In MX9116n, when snmpwalk is initiated to view the operStatus of the ports, the ports which are in "dormant" status are displayed as "down (2)" instead of "dormant (5)".
AR-42884	10.5.4.9	show counter output is missing from the sos report.
AR-42514	10.5.4.8	When the primary Radius server is unreachable, if you set the secondary Radius server key, it is using the primary Radius server key.
AR-42122	10.5.4.8	For a new login session using TACACS authentication over management VRF, the OS10 switch sends the loopback IP as the remote IP address to the TACACS server.
AR-42952	10.5.4.8	In certain scenarios, the BGP Up timer is counting down.
AR-42405	10.5.4.8	400G CR8 DAC cable from a third party is recognized as the 100G CR4.
AR-42149	10.5.4.8	The switch reboots when we try to negate an existing domain name in IP DHCP config mode.
AR-43063	10.5.4.8	When DHCP broadcasts the packet with snooping enabled and without DHCP option 82, it floods all the VLT port channel member ports and VLTi from applications.
AR-42939	10.5.4.8	The S5248F-ON device has two double-density ports (49, 50, and 51, 52), and each double-density port will have one PHY media port. If a user requests transceiver information using the show interface phy-eth command, the output is displayed incorrectly.  NOTE: This issue is only seen on the S5248F-ON switch.
AR-42746	10.5.4.8	Memory leaks are observed when LLDP is enabled on directly connected devices.
AR-42134	10.5.4.8	Rest call to /data/interfaces-state/interface returns broken output for unsupported management address subtypes.
AR-42342	10.5.4.8	Restconf request for local mac-address and local port-id information displays the value in encoded format.
AR-43117	10.5.4.8	In nondefault VRF with VLT peer routing, a BFD, BGP, or OSPF session to a VLT node through a VLT-LAG, may go down if links in that VLT-LAG towards that VLT-Node go down.  NOTE: This issue is only seen on the S5432 and Z9432F-ON switches.

Table 4. Previous resolved issues (continued)

Issue ID	Resolved in	Description
AR-42790	10.5.4.8	When you run the <code>show processes</code> command, it displays NaN in the output due to a <code>dn_pm</code> process crash.
AR-42653	10.5.4.8	When the VLT lag is in MSTP mode, the STP cost, and priority values are reset to their default values after reboot.
AR-42865	10.5.4.8	IP reachability track object is not working on nondefault VRFs after a reboot.
AR-42796	10.5.4.8	When advertising routes using OSPF to a switch, it reports that the 128.0.0.0/1 route is not installed in the routing table.
AR-42533	10.5.4.8	When the device with a 400G DAC is reloaded, some of the links go down randomly. NOTE: This issue is only seen on the Z9432F-ON switch.
AR-42816	10.5.4.8	Packet loss occurs when 1GBaseT, 1GBase-SX, or 1GBase-LX optic is used in one of the SFP+ ports. NOTE: This issue is only seen on the N3248TE-ON switch.
AR-43079	10.5.4.8	<ul style="list-style-type: none"> Event alarms are incorrectly raised during control plane policer configurations due to accounting errors in total and configured policer values. When multiple control plane class maps are configured, <code>show running configuration</code> incorrectly displays all the class map match policies instead of the current class map match policy. NOTE: This issue is only seen on the S4128F-ON, S4128T-ON, S5224F-ON, S5232F-ON, S5248, S5248F-ON, and Z9432F-ON switches.
AR-42299	10.5.4.8	Hosts are unreachable after the /32 host route is added.
AR-42771	10.5.4.8	When PBR is used with two next hops to accomplish routing redundancy, if the primary next-hop is unavailable, the routing switches to the secondary next-hop. However, when the primary next hop is restored, fallback to the primary next hop does not happen.
AR-42884	10.5.4.8	<code>show counter</code> output is missing from the <code>sosreport</code> .
AR-43124	10.5.4.8	When both sender and receiver are in the same VLAN with snooping enabled, multicast packets drop.
AR-42474	10.5.4.8	Local users can still log in to the device after running the <code>delete startup-configuration</code> command.
AR-42656	10.5.4.8	Trap syslog does not have the OID information about <code>warmStart</code> or <code>coldStart</code> .
AR-42553	10.5.4.8	<code>snmpwalk</code> for <code>sysServices</code> (OID .1.3.6.1.2.1.1.7.0) shows an incorrect value.
AR-42646	10.5.4.8	Unable to configure SNMPv3 traps.
AR-42243	10.5.4.8	<code>AuthoritativeEngineBoots</code> and <code>AuthoritativeEngineTime</code> values in SNMPv3 traps are not getting incremented.
AR-43061	10.5.4.8	Compilation errors are seen in the Dell SNMP MIB files.
AR-42645	10.5.4.8	The value for discarded packets (egress) in the <code>show interface [type]</code> command displays an incorrect value. NOTE: This issue is only seen on the S5232F-ON, S5248F-ON, S5296F-ON, S5212F-ON, and S5224F-ON switches.
AR-42928	10.5.4.8	After a reload, sometimes <code>vlan2</code> is in a bad state. unable to delete, re-create, or modify <code>vlan2</code> .
AR-42250	10.5.4.8	Some of the VLANs information is incorrect after the upgrade from 10.5.1.6 to a higher release.
AR-40896	10.5.4.8	During the ZTD process, the post configuration is not fully loaded in rare cases.
AR-42876	10.5.4.7	Fetching the MAC address using the SNMP MIB returns an error when port security is enabled and <code>sticky</code> or <code>mac-learn disable</code> is configured.

Table 4. Previous resolved issues (continued)


Issue ID	Resolved in	Description
AR-41929	10.5.4.5	<code>snmpwalk</code> does not show MIBs for the fan status when the fan tray or PSU is removed.
AR-42353	10.5.4.5	OS10 switches running 10.5.4.2 or later cannot be registered to the SupportAssist server using OMNI, SFS, and REST API.
AR-42471	10.5.4.5	If you have configured SupportAssist to connect to an Secure Remote Services server using Secure Connect Gateway, upgrading from 10.5.4.0 to 10.5.4.1 or later will result in a loss of connectivity to the Secure Remote Services server. This issue is also applicable when you reload the OS on the switches running 10.5.4.1 or later.
AR-41584	10.5.4.4	DHCP relay is not working in a specific topology.
AR-42297	10.5.4.4	For BMC-based platforms, PSU and fan tray information are shown as "NA" in the output when using the <code>show inventory</code> command.
AR-41704	10.5.4.4	The fan led shows the incorrect status of the fan tray.  NOTE: This issue is only seen on the N3248TE-ON and N3224F-ON switches.
AR-41930	10.5.4.4	When you copy the active image to the standby partition using the <code>image copy active-to-standby</code> command, the switch configuration is not synced to the standby partition.
AR-41970	10.5.4.4	VxRail switches in SmartFabric mode have an incorrect threshold value of free memory, which results in a memory alarm.
AR-42059	10.5.4.4	When the switches are in a VLT pair, the secondary switch of the VLT pair reboots due to the <code>dhcrelay</code> crash.
AR-42195	10.5.4.4	The following CVE have been addressed: <ul style="list-style-type: none"> ● CVE-2022-1012 ● CVE-2022-32296 ● CVE-2022-21123 ● CVE-2022-21125 ● CVE-2022-21166 The CVE database can be accessed here: CVE Org .
AR-41646	10.5.4.4	The SSH session is terminated when you run the CLI command <code>show lldp neighbors</code> .
AR-41913	10.5.4.4	PIM Register is not forwarded when the packet size is greater than the configured MTU of the egress interface.
AR-42183	10.5.4.4	When you configure the spanning-tree mode using the <code>spanning-tree mode rstp</code> command and save the configuration, sometimes the configuration mode changes back to the default setting of <code>rapid-pvst</code> after a reload.
AR-41138	10.5.4.4	SCG (Secure Connect Gateway) 5.0 shows as failed for the PowerSwitch in the <code>Status</code> section on the <code>Manage device</code> page.
AR-40755	10.5.4.4	When VLT LAG is down and comes up, the proxy ARP response is sent back on the same VLT LAG interface for approximately 10 s.
AR-42218	10.5.4.3	The connection status is disabled, and devices will not onboard when you configure the new devices running 10.5.4.2 to the SupportAssist server.
AR-41644	10.5.4.3	When you shut down multiple VLT Lags in one of the VLT nodes using the <code>interface range</code> command, you see traffic loss across the VLT Lags.
AR-41742	10.5.4.3	When you power off multiple remote devices that are connected to VLT lags and have a short LACP timeout configuration, this affects other VLT lag aggregations that are connected to the active servers. The fix is available for powering off up to 10 servers without affecting other VLT Lag aggregations.
AR-42009	10.5.4.2	When the switch connects to the Secure Remote Services server, the Secure Remote Services certificates that OS10 validates expire on January 15, 2023. After expiration, the connection cannot be established, and the SupportAssist feature will not be usable.

Table 4. Previous resolved issues (continued)

Issue ID	Resolved in	Description
AR-40938	10.5.4.2	Unable to remove the L2QOS policy from the interface when the QOS-ACL table entries exceed the allowed limit.
AR-41396	10.5.4.2	The untagged vlan is not correctly configured in the hardware under certain conditions, resulting in a failure to reach the VRRP IP.
AR-41557	10.5.4.2	ERSPAN session creation fails when the configured destination IP is reachable using a VLAN interface which is tagged to a port channel.
AR-41612	10.5.4.2	LACP PDUs are sent out through VLT Lag from the switch side when the VLT Lag is in fallback active mode.
AR-41725	10.5.4.2	Snmpwalk shows incorrect values for OID <i>os10FanOperStatus</i> .
AR-41743	10.5.4.2	System chooses the static route over OSPF even if the static route has a higher Administrative Distance(AD).
AR-41774	10.5.4.2	In certain scenarios, the switch experiences an unexpected crash while checking the port status.
AR-41833	10.5.4.2	The management console displays the error message "The operational status of the I/O Module identified in the message has ended".
AR-40450	10.5.4.2	If the admin password has the @ symbol in the passphrase, the module replacement script fails.
AR-41099	10.5.4.2	Some interfaces may go missing from the <code>show brctl</code> command output and MAC addresses are not learned on the interface after upgrading to 10.5.4.0.  NOTE: This issue is only seen on the S4148T-ON switches.
AR-41869	10.5.4.2	Restoration of Sticky-MACs present in the CPS DB is failing, which might cause a system crash while upgrading from 10.5.2.
AR-39857	10.5.4.2	The switch sends the router link state update with a wrong source IP if the OSPF router Link State Advertisement (LSA) update is greater than the link MTU.
AR-41078	10.5.4.2	Bringing down a BFD enabled interface fails to generate a syslog message.
AR-41113	10.5.4.2	When the VLT port channel interface is down on node 1, and the peer VLT node (node 2) reloads, host MAC entries that are learned on node-2 of the VLT port channel do not get programmed in the node 1 kernel.
AR-41242	10.5.4.2	Load-balancing configuration is inconsistent after a reload.
AR-41260	10.5.4.2	When performing an snmpwalk for OID 1.3.6.1.2.1.2.2.1.3 [Interface Type], snmpwalk fails to display the output of interface entries from the first virtual network interface.
AR-41144	10.5.4.2	Optic reports no power on Tx for QSFP-28 100G media as there is no check to display the Tx power values.
AR-41258	10.5.4.2	Port channel creation fails when the default VLAN is 1024.
AR-41478	10.5.4.2	Port breakout fails when the number of ports is more than 128.
AR-34127	10.5.4.2	When AAA accounting is enabled using the <code>aaa accounting commands all console start-stop logging</code> command, the commands that are configured by the user are not logged in the log-file.
AR-41626	10.5.4.2	Unable to disable the server logging using the <code>no logging server <ip-address></code> command. It shows the error "Could not config host or IP address" when the logging server vrf management is configured.
AR-41926	10.5.4.2	snmpwalk shows an incorrect sequence of fan status values.
AR-42007	10.5.4.2	Tx optical power values for QSFP+ and QSFP28 optics are not displayed.
AR-41922	10.5.4.2	Assigning VLANs to interfaces or creating new VLANs can fail in Smart Fabric mode.

Table 4. Previous resolved issues (continued)




Issue ID	Resolved in	Description
AR-42158	10.5.4.2	System reboots due to dn_app_iscsi_op process memory leak.
AR-41000	10.5.4.0	REST API CLI is not translated as expected for the following commands: <ul style="list-style-type: none"> • <code>aaa accounting commands all default start-stop logging</code> • <code>snmp-server host \$IP trap version 2c community</code>
AR-41445	10.5.4.0	The <code>show vrrp brief</code> command is not displaying the operational priority.
AR-41549	10.5.4.0	Update CPLD version in 'show system' output as per Inclusive Language.
AR-41490	10.5.4.0	The following CVE has been addressed: <ul style="list-style-type: none"> • CVE-2022-0778 The CVE database can be accessed here: CVE Org .
AR-41404	10.5.4.0	When ARP suppression is enabled, duplicate IP can lead to CPU spike, memory depletion, and eventual reboot of the system.
AR-39839	10.5.4.0	Multiple fabric validation warnings do not get cleared even after the configurations are synced and stabilized. There is no functionality impact.
AR-41006	10.5.4.0	Power details display as zero in the <code>show interface phy-eth transceiver</code> command output. There is no functionality impact, the optics that is connected to the ports are OPER UP, and all media settings and other show outputs are correct. <p> NOTE: This issue is only applicable to the S5448F-ON switch.</p>
AR-41324	10.5.4.0	Auto break-out fails if more than two ports are present in the <code>hybrid-port-group</code> instance. <p> NOTE: This issue is only seen on the S5448F-ON, Z9332F-ON, and Z9432F-ON switches.</p>
AR-41343	10.5.4.0	When trying to validate the S5448F-ON switch, it shows as unsupported in SmartFabric services. <p> NOTE: This issue is only seen on the S5448F-ON switch.</p>
AR-41145	10.5.4.0	The switch allows static multicast MAC configuration incorrectly.
AR-41244	10.5.4.0	Load balancing fails when the <code>tcp-udp-selection</code> configuration is changed.
AR-40990	10.5.4.0	The switch may encounter an exception when the BGP aggregate prefix matches with two or more BGP learned prefixes.
AR-41098	10.5.4.0	When an SNMP walk for the BGP peer table is performed, many OIDs go missing.
AR-41165	10.5.4.0	The <code>show inventory media</code> command output must not display the Qualified column.
AR-41198	10.5.4.0	A temporary traffic loop may be seen when the VLT interconnect link flaps along with the VLT heart-beat going down.
AR-41310	10.5.4.0	A "dictionary changed size during iteration" runtime error may occur if python 3 is used for IPv6 Duplicate Address Detection.
AR-40628	10.5.4.0	While enabling DHCP Snooping, the switches may undergo an unexpected reboot due to possible memory leak.
AR-40416	10.5.4.0	In certain scenarios, the switch may encounter a software exception while configuring PBR.
AR-40881	10.5.4.0	While using Controller Provisioned VXLAN, the switches may undergo unexpected reboot due to possible memory leak in vtep process.
AR-41319	10.5.4.0	When using the <code>password-attributes character-restriction special-char</code> command to set password attributes, it does not allow the setting of the number of special characters.
AR-41246	10.5.4.0	While polling the OSPF MIB to get the <code>ospfAread</code> object, the switch adds an extra value of 06 in the OID reply.

Table 4. Previous resolved issues (continued)

Issue ID	Resolved in	Description
AR-40241	10.5.4.0	When reconfiguring the virtual-network, remote-vtep, and vxlan-vni commands, there may be a mismatch between MAC addresses that are learned in the actual hardware, and the show mac-address virtual-network command output.
AR-41127	10.5.4.0	The following CVE has been addressed: <ul style="list-style-type: none"> • CVE-2022-29089 The CVE database can be accessed here: CVE Org .
AR-41833	10.5.4.0	The management console displays the error message "The operational status of the I/O Module identified in the message has ended".
AR-41167	10.5.4.0	Holdover takes longer than expected when the G8275.2 profile is in use.

Known issues in 10.5.4.10

The following high severity issues remain unresolved in this release.

Table 5. Known issues


Issue ID	Functional Area	Description	Workaround or Resolution
AR-43224	SAI-BCM	When the device is loaded or connected with 400G Optics for more than 16 ports, the device gets stuck in the "system is loading" status.  NOTE: This issue is only seen on the Z9664F-ON switch.	N/A
AR-43074	SNMP	In SNMP, an incorrect OID value is displayed in the BGP Established and BGP BackwardTransition Trap messages.	N/A
AR-41049	DHCP	The default DHCP gateway overrides the default VRF management route and the non-vrf management route.	N/A
AR-43037	SNMP	When the "snmp-sever vrf default" command is run for the first time, an error that is failed to enable VRF is displayed.	N/A
AR-42284	Syslog-NG	The Fully Qualified Domain Name (FQDN) configuration for remote logging server is not working in the nondefault and management VRFs.	Use IP address configuration instead of FQDN.
AR-43230	Logging	When the device authentication over the management VRF fails, the syslog is updated with the VRF IP address 127.100.x.x instead of the actual IP address of the device.	N/A
AR-41797	VRRP	When you modify or delete the IPv6 link local address of the VRRP configured interface, the IPv6 VRRP becomes inconsistent.	Remove and add the VRRP v6 configuration.
AR-42277	SupportAssist	When the OS10 system's clock is configured or adjusted backwards, full transfer and performance transfer operations are not successful.	After you configure or adjust the system clock of OS10 backwards, reconfigure the SupportAssist by running the below commands in sequence. <ul style="list-style-type: none"> • eula-consent support-assist reject • eula-consent support-assist accept

Table 5. Known issues (continued)

Issue ID	Functional Area	Description	Workaround or Resolution
			<ul style="list-style-type: none"> • <code>support-assist</code> • <code>server url default</code> • <code>support-assist generate universal-key <access-Key> <pin></code> <p>NOTE: Generate the universal key by using the new access-key and PIN values from the connectivity portal.</p>
AR-41219	VLAN	Configuring VLAN assignments in transaction mode may not work.	Configure VLAN assignments in nontransaction mode.
AR-42231	PAS Media	While performing OIR for the cables listed below, there is a one-time link flap at the breakout end: <ul style="list-style-type: none"> • 400 GbE QSFP56-DD to 4x100G depop-Q56 copper DAC breakout cable. • 400G QSFP56-DD to 2x200G QSFP56-SFF DAC breakout cable. 	Interface links work fine after one-time flap.
AR-42220	PAS Media	Interface links are not coming up after break-in to 400g-1x native speed.	Links will come up after running the below commands in sequence. <ul style="list-style-type: none"> • <code>shutdown</code> • <code>no shutdown</code>
AR-39782	Management services	The <code>running-configuration</code> timestamp gets updated on every new session that is opened, without any configuration changes being performed.	Configure the <code>no service obscure-password</code> command.
AR-40149	SNMP	When an encrypted password is copy pasted in the <code>snmp-server user</code> command or running config, the command fails to function as expected.	The encrypted password must be saved and loaded through the startup config.
AR-43129	SAI	The traceroute feature is not working with the UDP protocol.	Configure the <code>switchport mode access</code> command.
AR-40521	VXLAN	A traffic loop may occur if egress ACL is applied on network facing ports in a VTEP with <code>permit</code> rule matching any Broadcast, Multicast, or Unknown-unicast traffic that flow over VXLAN tunnels. <p>NOTE: This issue is only seen on the S5448F-ON PowerConnect switch.</p>	Do not configure egress ACL on network-facing ports on VTEPs.
AR-40677	Routing	If the reserved IPv6 subnet (<code>fde1:53ba:e9a0:cccc::/64</code>) IP address is used for data virtual networks (VN) in any of the nodes which are part of a cluster, and that node becomes the master or if the node is reloaded and becomes the master, cluster connectivity, or data VN Connectivity may be lost. <p>NOTE: This issue is only seen on the S4100-ON Series, S5200-ON Series, Z9100-ON, Z9264F-ON, and Z9432F-ON switches.</p>	Unconfigure the reserved IPv6 address from the data VN and configure an IPv6 address from another subnet.

Table 5. Known issues (continued)

Issue ID	Functional Area	Description	Workaround or Resolution
AR-40685	VxRail	When the admin status of a server-connected interface is explicitly enabled using the SFS UI, OMNI UI, or REST APIs, there may be traffic loss on those ports when the node is reloaded. i NOTE: This issue is only applicable to the VxRail solution.	Do not configure admin state for the server port from the SFS UI, OMNI UI, or REST API.
AR-39385	VXLAN	In the Z9432 platform, when an ingress QOS policy-map configuration is applied on an access port interface with action to set the DSCP in the IP header, then for traffic incoming on that access port that is destined to remote VTEP, DSCP marking shall be done only on the outer IP header, the inner IP header may not be DSCP marked. i NOTE: This issue is only seen on the Z9432F-ON switch.	N/A
AR-34906	VLT	With Static VLT LAG configured, a transient loop can occur whenever a VLT node is reloaded.	Instead of using static LAG, LACP could be used.
AR-40608	VXLAN	With ARP suppression enabled, ARP or neighbor entries on virtual-network interfaces may not be synchronized with VLT peers after running the clear ip arp command on VLT peers.	ARP or neighbor entries are learned automatically when data traffic, ARP, or neighbor resolution packets hash to the VLT peer. No action is needed.
AR-42187	VxRail	Validation error is reported for unused PCIE card interfaces during Day-0 Deployment with VxRail.	Ignore the validation error and proceed.

Installation

⚠ WARNING: When upgrading from OS10.4.3.x to OS10.5.x.x, ensure that all pre-requisites are met before starting the multi-step upgrade process.

For complete installation and upgrade information using the ONIE installer, follow the instructions in the [Dell SmartFabric OS10 Installation, Upgrade, and Downgrade Guide](#).

See [Dell SmartFabric OS10 Documentation page](#) to download this guide.

PowerEdge MX Installation Instructions

i **NOTE:** OS downgrade or rollback is not recommended for MX-series switches.

See the *OS10 Firmware Update Matrix* section in the latest version of the [Dell OpenManage Enterprise-Modular Edition for PowerEdge MX7000 Chassis User's Guide](#) for instructions to update the MX9116n Fabric Switching Engine, and MX5108n Ethernet switch to the latest version.

For additional information about PowerEdge MX Networking, see the [Dell Infohub](#).

Support resources

The Dell support site provides a range of documents and tools to assist you with effectively using Dell devices. Through the support site you can obtain technical information regarding Dell products, access software upgrades and patches, download

available management software, and manage your open cases. The Dell support site provides integrated, secure access to these services.

To access the Dell support site, go to [Dell Support](#). Sign in with a previously created account or create an account. To display information in your language, scroll down to the bottom of the page and select your country or region from the drop-down menu.


- To obtain product-specific information, enter the 7-character service tag or 11-digit express service code of your switch and click **Submit**. To view the service tag or express service code, pull out the luggage tag on the chassis or enter the `show chassis` command from the CLI.
- To submit service requests or to contact technical support by phone or chat, click **Contact Us**, and then click **Technical Support**.

To access product documentation and resources that might be helpful to configure and troubleshoot the OS10 Networking operating system, see the [Dell Networking OS10 Info Hub](#).

To search for drivers and downloads, see the [Dell SmartFabric OS10 Drivers page](#).

To participate in Dell community blogs and forums, see the [Dell Community page](#).

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.