FortiNAC - Release Notes

Version F 7.4.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 26, 2024
FortiNAC F 7.4.0 Release Notes
49-922-769106-20211216

TABLE OF CONTENTS

Change log

Date	Change description
February 26, 2024	Initial release.

Overview of Version F 7.4.0

- Build number: 0427

Notes

- Starting from 9.1.0, FortiNAC uses a new GUI format. FortiNAC cannot go backwards to a previous version. Snapshots should always be taken on virtual appliances prior to upgrade.

Post 9.4, FortiNAC re-versioned. The first release after re-versioning is F 7.2.0. Hence, the order of releases is:

FortiNAC 9.1 > FortiNAC 9.2 > FortiNAC 9.4 > FortiNAC F 7.2 > FortiNAC F 7.4

- Prior to upgrading, review the FortiNAC Known Anomalies posted in the Fortinet Document Library.
- If using agents or configured for High Availability, additional steps may be required after upgrade for proper functionality. See Upgrade Instructions and Considerations posted in the Fortinet Document Library.
- For upgraded FortiNAC devices running CentOS, use the sysinfo command; for newly deployed FortiNAC F 7.4+, issue `get system status` within the admin CLI.
- To review software version information via CLI:

  Appliances running on CentOS: type `sysyinfo`

  Appliances running on FortiNAC-OS: type `get system status`
- For upgrade procedure, see Upgrade Instructions and Considerations posted in the Fortinet Document Library.

Supplemental Documentation

The following can be found in the Fortinet Document Library.

- FortiNAC Release Matrix

Version Information

These Release Notes contain additional Enhancements, Device Support, and features. Unique numbering is used for the various components of the product. The software version and Agent version supplied with this release are listed below.

Version: F 7.4.0

Agent Version:

- MacOS — 10.7.1.9
- Windows — 9.4.3.100

Agents ship independent of product. For the latest Agent release notes, please see the Agent release notes.

- MacOS — 10.7.1.9
- Windows — 9.4.3.100

A newer Persistent Agent may be required to support certain antivirus and anti-spyware products. Refer to the Agent Release Notes in the Fortinet Document Library.

Firmware version represents a collection of system services and operating system features imaged on to the appliance before it leaves manufacturing. The firmware image cannot be updated by a Fortinet customer. Services within the image are updated by Fortinet or a certified Fortinet Partner in appliance maintenance packages released as new more robust and secure versions of services become available.

Note: Upgrading software versions does not change firmware nor does it automatically require an upgrade to the Persistent Agent. Newer Persistent Agents are not compatible with older software versions unless that capability is specifically highlighted in the corresponding release notes.

Upgrade Requirements

Ticket #	Description
931408	Under **Portal > Portal SSL** the "Disabled" option is no longer available as of FortiNAC v9.4.5, vF7.2.5 and vF7.4.0. If using this option, install SSL certificates in the Portal target prior to upgrade. See Certificate management in the Administration Guide.
FortiNAC License Key	Upgrading to this release requires the FortiNAC License. It is possible, however unlikely, older appliances may not have this specific type of license key installed. In such cases, an error will display during the upgrade. For additional details, see KB article https://community.fortinet.com/t5/FortiNAC/Troubleshooting-Tip-Upgrade-fails-with-license-requirement-error/ta-p/246324
892856	High Availibility and FortiNAC Manager Environments: The following are required as of 7.2.2: Key files containing certificates are installed in all FortiNAC servers. License keys with certificates were introduced on January 1st 2020. Appliances registered after January 1st should have certificates. To confirm, login to the UI of each appliance and review the System Summary Dashboard widget (Certificates = Yes). If there are no certificates, see Importing License Key Certificates in the applicable FortiNAC Manager Guide. Allowed serial numbers: Due to enhancements in communication between FortiNAC servers, a list of allowed FortiNAC appliance serial numbers must be set. This can be configured prior to upgrade to avoid communication interruption. For instructions, see What's New.
834826	As of FortiNAC versions 9.4.2 & vF7.x, Persistent Agent communication using UDP 4567 is no longer supported. It is recommended the following be checked prior to upgrade to avoid agent communication disruptions: • SSL certificates are installed for the Persistent Agent target • Persistent Agents are running a minimum version of 5.3 For additional details see KB article 251359. https://community.fortinet.com/t5/FortiNAC/Technical-Note-Agent-communication-using-UDP-4567-no-longer/ta-p/251359
885056	All devices managed by FortiNAC must have a unique IP address. This includes FortiSwitches in Link Mode: Managed FortiSwitch interface IP addresses must be unique. Otherwise, they will not be properly managed by FortiNAC and inconsistencies may occur. This is also noted in the FortiSwitch Integration reference manual.

Upgrade path

Important notice

Version 9.1.7 may directly upgrade to 7.x, without any intermediary steps.

However, Version 9.1.6 *must* follow this path:

9.1.6 > 9.2.6 > 7.x

Current Version	Target Version	Upgrade Path Requirement	Ticket #
9.1 9.2 9.4 7.2	7.4	None	N/A
9.1 9.2 9.4	7.2	None	N/A
9.1 9.2 9.4	9.4	None	N/A
9.1.6	9.2	9.2.4 or higher	798530
8.2 or lower	8.4 or higher	Upgrade to 8.3 first	

Hardware support

FortiNAC-OS is supported on legacy hardware.

This section lists the hardware models supported by FortiNAC 7.4 F.

- FortiNAC-CA-500F: FN500F
- FortiNAC-CA-600F: FN600F
- FortiNAC-CA-700F: FN700F
- FortiNAC-M-550F: FN55MF
- FortiNAC-CA-500C: FN5HCA
- FortiNAC-CA-600C: FN6HCA
- FortiNAC-CA-700C: FN7HCA
- FortiNAC-M-550C: FN55M

Pre-upgrade Procedures

Enhancements were made to the communication method between FortiNAC servers for security. Due to this change, all servers must have additional configuration in order to communicate. The following procedure should be done prior to upgrade to prevent communication interruption.

Follow the instructions for the appropriate appliance:

- Pre-upgrade procedure (FNC-M-xx/FNC-CA-xx): FortiNAC appliances running on CentOS
- Pre-upgrade procedure (FNC-MX-xx/FNC-CAX-xx): FortiNAC appliance running on FortiNAC-OS

Pre-upgrade procedure (FNC-M-xx/FNC-CA-xx)

This configuration applies to FortiNAC version 7.2.2 and greater.

Configure all servers to allow communication between each other. This is done using an attribute that lists all the allowed serial numbers with which appliances can communicate.

Steps

1. Confirm key files containing certificates are installed in all FortiNAC servers.
   Administration UI Method:
   The **System Summary Dashboard** widget should show 'Certificates = Yes'.
   CLI Method:
   Virtual appliance: Log in to the CLI as root and type:

   ```
   licensetool
   ```

   Physical appliance: Log in to the CLI as root and type:

   ```
   licensetool -key FILE -file /bsc/campusMgr/.licenseKeyHW
   ```

   Response from the above commands should show:

   ```
   "certificates =[xxxxxxxxxxxxxxxxxx,xxxxxxxxxxxxxxxxxx]".
   ```

   If '`certificates = []`' or there is not a 'certificates' entry listed at all, keys with certificates must be installed. See Importing License Key Certificates in the FortiNAC Manager Guide.
2. Compile the allowed serial number list. In a text file (Notepad, etc), document the serial numbers of each appliance. Serial numbers can be obtained in the following ways:
   - Customer Portal (https://support.fortinet.com)
   - System Summery Dashboard widget in the Administration UI of each appliance
   - CLI of each appliance using licensetool command

   Example:
   FortiNAC Manager A (primary) & B (secondary)
   FortiNAC-CA servers A (primary) & B (secondary)
   FortiNAC-CA server C

Record serial numbers for:
FortiNAC Manager A: FNVM-Mxxxxx1
FortiNAC Manager B: FNVM-Mxxxxx2
FortiNAC-CA server A: FNVM-CAxxxxx4
FortiNAC-CA server B: FNVM-CAxxxxx5
FortiNAC-CA server C: FNVM-CAxxxxx6

3. In the same text file, write the following command, listing all the serial numbers recorded in step 2:
   Command:

   ```
   globaloptiontool -name security.allowedserialnumbers -setRaw
   "<serialnumber1>,<serialnumber2>,<serialnumber3>"
   ```

   Example

   ```
   globaloptiontool -name security.allowedserialnumbers -setRaw "FNVM-Mxxxxxxx1,FNVM-
   Mxxxxxxx2,FNVM-CAxxxxx4,FNVM-CAxxxxx5,FNVM-CAxxxxx6"
   ```

4. Perform the following steps on all servers:
   a. Log in to the CLI as root.
   b. Paste the `globaloptiontool` command from the text file.
   Note:
   - The message "Warning: There is no known option with name: security.allowedserialnumbers" may appear. This is normal.
   - In High Availability configurations, only the Primary Server need to have the command entered. Database replication will copy the configuration to the Secondary Server. Using the above example, CLI configuration would be applied to Manager A.

     Example

     ```
     > globaloptiontool -name security.allowedserialnumbers -setRaw "FNVM-
     Mxxxxxxx1,FNVM-Mxxxxxxx2,FNVM-CAxxxxx4,FNVM-CAxxxxx5,FNVM-CAxxxxx6"

     Warning: There is no known option with name: security.allowedserialnumbers

     New option added
     ```

   c. Confirm entry by typing:

   ```
   globaloptiontool -name security.allowedserialnumbers
   ```

   Example

   ```
   > globaloptiontool -name security.allowedserialnumbers

   Warning: There is no known option with name: security.allowedserialnumbers

   122 security.allowedserialnumbers: FNVM-Mxxxxxxx1,FNVM-Mxxxxxxx2,FNVM-
   CAxxxxx4,FNVM-CAxxxxx5,FNVM-CAxxxxx6
   ```

5. Log out of the CLI. Type:
   `logout`

You have completed the pre-upgrade procedure.

Pre-upgrade procedure (FNC-MX-xx/FNC-CAX-xx)

This configuration applies to FortiNAC version 7.2.2 and greater.

Configure all servers to allow communication between each other. This is done using an attribute that lists all the allowed serial numbers with which appliances can communicate.

Steps

1. Compile the allowed serial number list. In a text file (Notepad, etc), document the serial numbers of each appliance. Serial numbers can be obtained in the following ways:
   - Customer Portal (https://support.fortinet.com)
   - System Summery Dashboard widget in the Administration UI of each appliance
   - CLI of each appliance using get system status command

   Example:

   FortiNAC Manager A (primary) & B (secondary)

   FortiNAC-CA servers A (primary) & B (secondary)

   FortiNAC-CA server C

   Record serial numbers for:

   FortiNAC Manager A: FNVM-Mxxxxx1

   FortiNAC Manager B: FNVM-Mxxxxx2

   FortiNAC-CA server A: FNVM-CAxxxxx4

   FortiNAC-CA server B: FNVM-CAxxxxx5

   FortiNAC-CA server C: FNVM-CAxxxxx6
2. In the same text file, write the following command, listing all the serial numbers recorded in the previous step:

   Command:

   ```
   globaloptiontool -name security.allowedserialnumbers -setRaw
   "<serialnumber1>,<serialnumber2>,<serialnumber3>"
   ```

   Example

   ```
   globaloptiontool -name security.allowedserialnumbers -setRaw "FNVM-Mxxxxxxx1,FNVM-
   Mxxxxxxx2,FNVM-CAxxxxx4,FNVM-CAxxxxx5,FNVM-CAxxxxx6"
   ```
3. Perform the following steps on all servers:

   a. Log in to the CLI as admin and type:

   ```
   execute enter-shell
   ```

   Hit <ENTER>

   b. Paste the `globaloptiontool` command from the previous step.

   Note:
   - The message "Warning: There is no known option with name: security.allowedserialnumbers" may appear. This is normal.
   - In High Availability configurations, only the Primary Server need to have the command entered. Database replication will copy the configuration to the Secondary Server. Using the above example, CLI configuration would be applied to Manager A.

Example

```
> globaloptiontool -name security.allowedserialnumbers -setRaw "FNVM-
Mxxxxxxx1,FNVM-Mxxxxxxx2,FNVM-CAxxxxx4,FNVM-CAxxxxx5,FNVM-CAxxxxx6"

Warning: There is no known option with name: security.allowedserialnumbers

New option added
```

c. Confirm entry by typing:

```
globaloptiontool -name security.allowedserialnumbers
```

Example

```
> globaloptiontool -name security.allowedserialnumbers

Warning: There is no known option with name: security.allowedserialnumbers

122 security.allowedserialnumbers: FNVM-Mxxxxxxx1,FNVM-Mxxxxxxx2,FNVM-
CAxxxxx4,FNVM-CAxxxxx5,FNVM-CAxxxxx6
```

4. Restart FortiNAC services. Type:

```
shutdownNAC
```

<wait 30 seconds>

```
startupNAC
```

5. Log out of the CLI. Type:

```
exit

exit
```

You have completed the pre-upgrade procedure.

Compatibility

FortiNAC Product releases are not backwards compatible. It is not possible to go from a newer release to any older release.

Example: 7.2.0.0035 cannot be downgraded to any other release.

Agents

FortiNAC Agent Package releases 5.x are compatible with FortiNAC Product release F 7.4.0. Compatibility of Agent Package versions 4.x and below with FortiNAC F 7.4.0 is not guaranteed.

Web Browsers for the Administration UI

Many of the views in FortiNAC are highly dependent on JavaScript. The browser used directly impacts the performance of these views. It is recommended that you choose a browser with enhanced JavaScript processing.

Operating Systems Supported Without an Agent

Android	Apple iOS	Blackberry OS	BlackBerry 10 OS
Chrome OS	Free BSD	Kindle	Kindle Fire
iOS for iPad	iOS for iPhone	iOS for iPod	Linux
Mac OS X	Open BSD	Net BSD	RIM Tablet OS
Solaris	Symbian	Web OS	Windows
Windows CE	Windows Phone	Windows RT	

What's new

This section covers What's New for FortiNAC version F 7.4.

Version F 7.4.0

Radius CoA

Complete support for RADIUS Change of Authorization (CoA) with custom attributes (AVPairs).

- Full support for CoA messages as well as the standard "Packet of Disconnect."
- Ability to create a custom change of authorization profile which includes the required AVPairs / standard or vendor specific attributes to be sent in the CoA request message. This will allow the administrator to force a port bounce via RADIUS CoA message.
- Change of Authorization profile is assigned to the logical network.

See the RFC5176 CoA/Disconnect Message Cookbook.

EduRoam and Radius Service Proxy support

Support for an EduRoam environment with FortiNAC to create an authentication process for visitors from different institutions.

See the EduRoam Cookbook.

RADIUS Service Proxy Support / Deprecate existing (Legacy) Proxy

RADIUS service now supports the ability to proxy authentication requests and accounting packets to another server by creating a server configuration in the Virtual Servers tab of type 'Proxy'.

In pre-7.4 releases, the FortiNAC server itself would listen for and forward RADIUS packets rather than the RADIUS service. This has been deprecated. However, it can still be configured in the 'Legacy Proxy' tab.

SFTP

New SFTP backup feature provides an alternative to FTP backup that allows you to backup FortiNAC configuration by adding a layer of security to the process.

FortiNAC-F OS Migration support for FortiNAC legacy C-Series devices

The current FortiNAC appliances are built based on a Dell OEM hardware running with CentOS 7. FortiNAC CentOS 7 is coming to end-of-life by June 2024. In the near future, FortiNAC releases will only be available on FortiNAC-OS .

See the Hardware Migration Guide.

Agent enhancements

Persistent Agent Enhancements (Status Notification and User Acceptance)

Optionally include the current Logical Network name in the Status notification and tooltip for the Persistent Agent.

Optionally request the user to acknowledge VLAN changes through the Persistent Agent. Even in the case of no acknowledgement, the VLAN will be changed after a configurable timeout.

Support for Palo Alto XDR

Palo Alto XDR is now detected as an Anti-Virus product for Windows and macOS.

Support for Trend Micro Apex One (Japanese Version)

Trend Micro Apex One (Japanese Version) is now supported for Windows.

Device integration

FortiLAN Cloud - FortiAP and FortiSwitch support

User can now add FortiAP and FortiSwitch to FortiLAN Cloud; via service connector, the user can synchronize the devices information from FortiLAN Cloud.

See the FortiLAN page of the administration guide.

Support of Meraki MX as Radius Concentrator/Wireless Controller

See the Meraki MX Controller Wireless Integration Reference Manual.

Support for Claroty

See the Claroty page of the MDM integration guide.

Arista Cloud Wireless Integration

FortiNAC provides network visibility (where endpoints connect) and manages network access for wireless endpoints connecting to Access Points managed by the Arista Cloud Wireless Controller. FortiNAC supports individual SSID configuration and management for this device.

See the Arista Cloud Wireless Integration Reference Manual.

Custom windows registry scan to support date comparison logic

User can create a custom scan to compare registry date value.

See **Registry Date** under Windows Custom Scan.

HSTS default enabling

HSTS for the Admin GUI is enabled by default in versions 9.4.5+, 7.2.4+, and 7.4.0+.

Resolved Issues Version F 7.4.0

See also Resolved Issues for Versions:

- 9.2.8
- 9.4.5
- F 7.2.5

Ticket #	Description
981753	Discovery frequency check and discovery quantity check could be incorrectly done on single range when there are lists of ranges in one request. Moved the checking to the beginning of the request.
913595	Removed "Default" from Device/VDOM/SSID RADIUS Attribute Group label to avoid confusion with Logical Network attribute group.
990531	Migration script fails to bundle on Control and Application server pairs configured for High Availability.
932570	Unable to determine mibID when FirmwareVersion contains no suffix (e.g. FirmwareVersion = Huawei instead of Huawei.10). Causes operations requiring the mibID to fail (L2 Polling, reading SSIDs, etc).
955711	Guest account creation does not retain some account data.
901925	Removing profile mapping operation deletes the admin user account.
858184	Custom subject line for Self Registration Request sent to sponsor does not reflect custom text.
810574	Unable to scan using Dissolvable agent when scan configuration label contains non-US-ASCII characters.
972884	Config backup file taken before the FortiNAC factory reset cannot be restored after factory reset, and vice versa.
909376	FortiNAC-OS CLI: Unable to tail named.log file in CLI due to permissions.
907413	Include get hardware status and get system status in grab-log-snapshot.
906910	Include show full-configuration in grab-log-snapshot.
896471	Licensetool is not correctly reporting the license level from the NCM.
848851	hs_err_ files missing from grab log snapshot.
845008	Grab-log-snapshot should collect more master log files than the two collected.
969258	Config Wizard: Configuring an invalid Subnet Mask (255.255.225.0) on an Isolation Interface (Isol-Reg...) is accepted.
900281	Unable to add a scope in Config Wizard when Administration UI is

Ticket #	Description
	accessed through a port other than 8443.
881899	FortiNAC is unable to resolve hostnames unless they are fully qualified domain names (FQDNs).
987145	PlanetSwitch Port Switching using ifIndex instead of ifName.
986049	FortiSwitch MAC Trap Notifications not mapping to the correct switch port.
983350	Parsed VLAN is incorrect for Mist AP.
982255	Unable to gather L3 data on HPE 5130 Switch.
980338	When enabling authentication in MICROSENS G6 Micro-Switch port, the host information appears only in port 1.
977249	L2 poll not detecting 802.1x authenticated endpoints on NEC-QX switch.
974223	RADIUS support for NEC-QX switches.
956436	FortiNAC doesn't work as RADIUS proxy properly when integrated with NEC-QX switch.
954103	After FortiGate power cycle, FortiNAC shows incorrect port state for FortiSwitches (FortiLink) once the device is pingable again.
922095	Grab-Device-Debug does not successfully run due to permissions errors.
914193	Issues with Brocade switch - not seeing all VLANs and hence unable to set VLANs in model.
912128	FortiNAC is not sending CoA to Meraki MS switch on host state changes.
907854	VLAN change commands fail for Cisco SG-250.
904541	FirmwareVersion value missing from Meraki AP's on upgrade to 9.4.
900284	Juniper switches are taking longer than they should to make changes.
899075	Incomplete ARP table for Sonicwall appliance.
897851	FortiNAC not supporting QX series Mac-notification trap.
897151	Remove invalid device mapping for C9800-AP Software.
885306	WLC Extreme VX9000 MAC table can't be parsed.
882129	Meraki Switch doesn't populate data from L3 polling.
881650	HP J9776A 2530-24G Switch - uplink ports are not properly displayed in Ports view.
878102	FortiNAC not recognizing Extreme Wireless SSID.
874363	FortiGate VPN user not consistently retaining firewall tag when multiple connected adapters exist on the endpoint.
871657	Pnetworks newer Switches OS are using generic firewall OID.

Ticket #	Description
866343	Added proxy RADIUS support for Arista switches.
989711	Get error when import csv-file with host.expireDate.
981854	Registration Requests view is visible for admin users that do not have Host Registration Requests permissions.
980783	CLI Tool does not set Device Name completely.
977208	Override Scan Control doesn't work in latest GUI.
969091	Admin with System Administrator profile cannot delete another user in the UI with Base license.
969037	In the Adapters view in Ports tab, PA status will show the green tick when the agent hasn’t checked in.
956088	WebUI Session Timer not working.
951938	Admin Profile for Guest Permissions can see other accounts.
905865	Cannot enable 'Enable Quarantine VLAN Switching' option in GUI.
902533	Modifying port name value via port properties that include '&' generates 'amp;' in port name.
901257	HTML is not supported in the 'Guest Account details'.
897921	Firewall session polling does not get hostname.
894165	Test Device Profiling Rule results in 'Rule Does Not Match' if rule name contains a double space.
893561	Load CLI Configuration error when navigating to System > Scheduler.
890988	Device View in Inventory does not load for users with 'Network Devices->Access' read only permissions.
890929	Unable to restart server after uploading new license key through GUI.
890015	Can't edit the syslog files, 'filter values consisting of only alphanumeric characters'.
888616	Scheduler errors after upgrade from old versions 8.8.
887470	Domain with single character between dots in multiple dot domains results in error when adding to allowed domains.
884077	Guests & Contractors - Modifying a Guest account with 'Can view passwords:' permission disabled generates error.
883989	Default attribute for Phone is incorrect when adding an AD server to LDAP settings.
835149	Host role cannot be modified for endpoint registered as device in host and inventory view from within inventory/topology view.

Ticket #	Description
833305	Guest account password is unmasked on badge when user does not have password viewing permissions.
888212	Endpoint Compliance Scans are not replicated.
800870	If High Availability was re-configured with another FortiNAC Secondary Server, it is possible for the Primary Server to stop its processes if it receives communication from the original Secondary Server.
950004	Jamf MDM Integration - Need Bearer Token Authentication Support to Replace Basic Authentication.
919953	Enhance MSIntune Integration to query MSIntune API for a specific host on-demand. For details, see: https://docs.fortinet.com/document/fortinac-f/7.4.0/mdm-integration/825384/microsoft-intune
878836	Intune MDM Integration 'Invalid Audience' when using an App registration in the Azure Government cloud.
884986	Remove Log4j package.
992236	Device Profiling rule with WINRM method not matching properly.
944935	FortiNAC unable to start processes during a failover or resuming control in High Availability configuration
911631	Remove setupAdvanceRouting.
889125	FortiNAC Azure zip file appears to be corrupt.
982765	Proxy Radius validation and test and save function result in RADIUS reject due to incorrect password attribute.
978006	FortiNAC keeps sending disconnect-request with the old calling-station-ID even though it is connected to a new docking station.
918983	Additional Radius Attribute Groups applied to Logical Network misbehaving.
901236	Radius Authentication rejecting with network access policy setup with Direct configuration.
895085	RADIUS Performance problems on rogue host record creation.
864232	FortiNAC sends 2 Disconnect-Request after the device initially connects to Juniper/Nokia switches to determine the Correct Delimiter.
882265	FortiNAC is not sending the correct serial number field to FortiAnalyzer.
884345	REST API V2 error response.
909839	Repetitive SSO logon and logoffs.
902072	Improved DatabaseServer performance.

Ticket #	Description
882782	NullPointerException in MessagingGatewayPlugin.sendSMS().
877942	Performance issues related to Firewall Session table growing too large.
987991	"This Host name contained characters not allowed in host names" appears if the length of host.host in csv file is 2 characters.
986547	Port Changes view in Admin GUI showing incorrect values.
980366	Unable to connect to Admin GUI on secondary after starting secondary GUI service.
896150	Interfaces not properly mapped when installing FortiNAC-OS KVM image.

Known Issues Version F 7.4.0

Ticket #	Description
972925	OS information on device/adapter is not always accurate.
985653	Host/agent is connecting to FortiNAC despite having 'require connected adapter' feature enabled.
999354	Host remains isolated due to delay in Agent reporting external network connectors.
996251	FortiNAC-F is unable to profile PXE boot host since it does not build profiling/fingeprint entries from DHCP PXE boot packets.
994775	FortiNAC doesn't change the FortiGate/FortiSwitch port mode from 802.1x to Normal and vice-versa.
1002475	Unable to scan using Dissolvable Agent with spaces in scan name.
998758	Captive Portal Authentication Failure message "Custom text" not taking effect when customized via Portal Configuration.
998736	Syslog format changed in FortiGate Firmware 7.4.2 causing FortiNAC to not be able to parse MAC Add, Delete, and Move messages.
996006	API Calls failing to remove or update user records.
988244	"Portal" and "Persistent Agent" SSL certificates not included in Control and Application Server pair to FortiNAC-OS server migrations.
972501	Syslog messages are not sent to new external log server until restart of services is preformed.
962235	Can't schedule a task in scheduler to start at 00:00:00 or any time with 00 as the hour.
974270	Non fabric root FortiGate does not have dynamic tags after firmware update.
970135	Unchecking System > FSSO communication returns "There was an error processing this request" when saving.
954220	Unable to restore system backup files on FortiNAC-OS appliances.
951419	HTTPS Status 500 - Internal Server Error attempting to access model config from right click context menu.
955985	Extreme switch with 'description-string' in switchport config won't display connected adapters in GUI device model.
964841	Users & Hosts > Hosts GUI does not allow selection of bulk hosts in view.
827499	Show system interface does not accurately display port1/port2 IP sub Interfaces on FortiNAC-OS appliances.

Ticket #	Description

	Workaround: Navigate to System > Config Wizard > Summary or run the following commands in the CLI:
	`execute enter-shell`
	`ip addr`

827283	The Roaming Guest Logical Network is missing from the Model Configuration of FortiGate and possibly from other vendors.

Device Support Considerations

Ticket #	Description
730221	Stacked Meraki switches currently not supported. If required, contact sales or support to submit a New Feature Request (NFR).
548902	Management of wired ports on Aerohive AP-150W controlled by AerohiveNG is currently unsupported.
679230	Aruba 9012-US currently not supported.If required, contact sales or support to submit a New Feature Request (NFR).
7680531	Ubiquiti Gen2 Unifi switches (example: USW-16-POE) are currently not supported. If required, contact sales or support to submit a New Feature Request (NFR).
860546	L3 Polling currently not supported on Extreme Wireless Controllers
	At this time, integration with Juniper MAG6610 VPN Gateway is not supported.This includes Pulse Connect Secure ASA.
	At this time, integration with Cisco 1852i Controller is not supported due to the device's limited CLI and SNMP capability. For details, see related KB article 189545.
	At this time, integration with Ubiquiti AirOS AP is not supported.Ubiquiti AirOS AP does not have the necessary capabilities to allow for full integration with FortiNAC. The limitations are as follows: - No support for external MAC Authentication using RADIUS. - Limited CLI and SNMP capability. No ability to dynamically modify access parameters (ie. VLANs) for active sessions.
	At this time, Fortinet does not support wired port management for the Cisco 702W. The access point does not provide the management capabilities required.
	At this time, Fortinet is not able to support the Linksys LAPN600 Wireless-N600 Dual Band Access Point.
	Ports on Avaya Networks 4850GTS-PWR+ switches sometimes show "Not Connected" even though the port is active. This is due to multiple ports on the switch using the same MAC Address. This prevents NAC from correctly discerning which are "Connected" versus "Not Connected". There is no workaround.
	Device models for Avaya 4800 switches (and potentially other related models) only support SSH. Device models for Avaya Ethernet Routing Switches only support Telnet. Contact Support if the alternate protocol is required.

Device Support

See also Device Support for Versions:

- F 7.2.5
- 9.4.5
- 9.2.8

Ticket #	Description
981176	Intelligent IEC 61850-3 28-port rack mount managed Gigabit Ethernet switch with 4 slots.
996537	Extreme Networks Switch Engine (5420F-16MW-32P-4XE-SwitchEngine) Extreme Networks, Inc. C5G124-48 Rev 06.81.08.0005 Huawei AR617VW-LTE4EA Huawei Versatile Routing Platform Software VRP (R) software,Version 5.170 Cisco IOS Software [Bengaluru], IE3x00 Switch Software (IE3x00-UNIVERSALK9-M), Version 17.6.3 HUAWEI CloudEngine S5735-L-V2 Cisco IOS Software, S5700 Software (S5700-UNIVERSALK9-M), Version 15.2(7)E3 HPE Comware Platform Software, Software Version 7.1.070 Cisco IOS Software [Bengaluru], IE3x00 Switch Software (IE3x00-UNIVERSALK9-M) Industrial 8-P GbE RJ45 + 2-P GbE RJ45/SFP Combo L2 Plus Managed PoE Switch 08G20G2-08 Gigabit Ethernet Switch JetStream 8-Port Gigabit L2 Managed Switch with 2 SFP Slots Aruba R8Q71A 6200M 36G 12SR5 CL6 PoE 4SFP+ Sw ML.10.11.1021
911439	MICROSENS G6 Switch
984156	DGS-1210-48 2.00.011 JetStream 24-Port Gigabit Stackable Smart Switch with 4 10GE SFP+ Slots JetStream 24-Port Gigabit L2+ Managed Switch with 4 10GE SFP+ Slots Aruba JL722C 8360 24p 10G SFP/SFP+ and 2p 40/100G QSFP+/QSFP28 switch Aruba Instant On 1830 8G 4p Class4 PoE 65W Switch JL811A, InstantOn_1830_2.6.0.0 (75), Linux 4.4.120, U-Boot Cisco IOS Software [Cupertino], Catalyst L3 Switch Software (IE9K_IOSXE), Version 17.9.2, RELEASE SOFTWARE (fc2) Cisco IOS Software, S5700 Software (S5700-UNIVERSALK9-M), Version 15.2(7)E Aruba R8Q70A 6200M 48G CL4 PoE 4SFP+

Ticket #	Description
	FortiAP-U431F Cisco IOS Software, S5700 Software (S5700-UNIVERSALK9-M), Version 15.2(6)E2a HP Comware Platform Software, Software Version 5.20.99, Release 2110P02 HP 3600-24 v2 EI Switch 1620-24G Switch Software Version 5.20.99, Release 1113 Arista Networks EOS version 4.30.4M running on an Arista Networks CCS-720DT-48S-2 Brocade Communications Systems, Inc. ICX7250-24, IronWare Version 08.0.30fT213 CBS350-48FP-4X 48-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks Juniper Networks, Inc. ex4100-f-12p Ethernet Switch, kernel JUNOS 22.3R2-S2.9 Cisco IOS Software [Dublin], Catalyst L3 Switch Software (CAT9K_IOSXE) Aruba Instant On 1930 24G Class4 PoE 4SFP/SFP+ 370W Switch JL684B
924265	Huawei Versatile Routing Platform Software VRP (R) software, Version 8.100 Cambium cnPilot E400 Access Point Huawei Versatile Routing Platform Software VRP (R) Software, Version 5.170 Aruba Instant On 1830 24G 12p Class4 PoE 2SFP 195W Switch JL813A S5710-28C-EI Huawei Versatile Routing Platform Software VRP (R) software,Version 5.110 Huawei AR2220 Huawei Versatile Routing Platform Software VRP
915803	ExtremeXOS (X465-24MU-24W) version 32.3.1.11 NetVanta 1234 PoE, Version: R13.10.2 SF350-48P 48-Port 10/100 PoE Managed Switch Cisco 48-port 10/100/1000 Ethernet Switch with PoE Cisco 24-port 10/100/1000 Ethernet Switch with PoE
898891	Cisco IOS Software [Bengaluru], c8000be Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.6.5 Cisco IOS Software, ir800 Software (ir800-UNIVERSALK9-M), Version 15.9(3)M5 Cisco IOS Software [Cupertino], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9_IOT-M), Version 17.9.1

System Update Settings

1. In the FortiNAC Administrative UI, navigate to **System > Settings > Updates > System**.
2. Update the appropriate fields to configure connection settings for the download server.

Field	Definition
Host	Set to fnac-updates.fortinet.net
Auto-Definition Directory	Keep the current value.
Product Distribution Directory	Set to Version_F7_4
Agent Distribution Directory	Keep the current value.
User	Set to updates (in lowercase)
Password	Credentials required. Default is not available.
Protocol	Set to desired protocol (FTP, PFTP, HTTP, HTTPS) Note: SFTP has been deprecated and connections will fail using this option. SFTP will be removed from the drop down menu in a later release.

3. When the download settings have been entered, click **Save Settings.**

Numbering Conventions

Fortinet is using the following version number format:

<First Number>.<Second Number>.<Third Number>.<Fourth Number>

Example: F 7.4.0.0427

- First Number = major version
- Second Number = minor version
- Third Number = maintenance version
- Fourth Number = build version

- Release Notes pertain to a certain version of the product. Release Notes are revised as needed. The Rev letter increments accordingly. For example, updating the Release Notes from Rev C to Rev D indicates changes in the Release notes only -- no changes were made to the product.