FortiNAC - Upgrade Instructions and Considerations

Version 9.x

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

FORTINET VIDEO GUIDE
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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

March 22, 2021
FortiNAC 9.x Upgrade Instructions and Considerations
49-900-000000-20210322

TABLE OF CONTENTS

Overview

This document provides the steps to upgrade the FortiNAC appliance software. For fixes/enhancements and device support details, refer to the applicable version of Release Notes in the Fortinet Document Library.

Procedure Overview

1. Review the following documentation before proceeding:
   Known Anomalies
   https://docs.fortinet.com/document/fortinac/8.3.7/known-anomalies
   Upgrade Considerations
   https://docs.fortinet.com/document/fortinac/8.6.0/upgrade-instructions-and-considerations/046354/upgrade-considerations
2. Virtual FortiNAC appliances: Run snapshot on each appliance to be upgraded.
   NOTE: FortiNAC cannot go backwards to a previous version
3. Run operating system updates and reboot appliance(s). For instructions, see CentOS Updates in the Fortinet Document Library.
   https://docs.fortinet.com/document/fortinac/8.3.0/fortinac-centos-updates
4. Upgrade software on the appliance(s).
   See Upgrade Instructions.
   https://docs.fortinet.com/document/fortinac/8.6.0/upgrade-instructions-and-considerations/921445/upgrade-instructions

Upgrade Considerations

1. FortiNAC cannot go backwards to a previous version
2. The use of SFTP has been deprecated. The SFTP option in the System Update Settings will be removed in a future release.
3. During the upgrade, FortiNAC automatically restarts its processes. The amount of time for the restart to complete depends upon the size of the database (typically between 5-10 minutes).
   During this time:
   - FortiNAC stops responding to RADIUS requests (wireless clients will be unable to connect)
   - Captive portal is unavailable (isolated devices will be unable to register or remediate)
   - VLANs stop switching
   - Wireless clients already connected are unaffected
   - Wired devices in production VLANs are unaffected
4. Systems may have specific configurations that are not persistent through an upgrade. Attempting to upgrade via the Administration UI will trigger an alert and the upgrade will not proceed. In such situations, a support ticket should be opened to schedule the upgrade.

Feature Specific Considerations

Version	Description
8.x	Upgrade path requirements: • Systems on version 7 must upgrade to 8.0 before upgrading to 8.1 or higher. • No intermediate upgrades are required from 8.0 to any other 8.x version.
8.x	Upgrading NAC from pre-8 versions to 8.x could break communication with agents running version 3.0 through 3.2. Hosts that have security disabled are not affected. In newer agent versions 3.3 and greater, the communication protocol was changed from SSLv3 to TLS to address the POODLE vulnerability (CVE-2014-3566). As of Network Sentry 8.0.0, SSLv3 has been disabled completely. Secure Agent Communication Compatibility Summary NAC 7.x: Compatible with all 3.x agents NAC 8.x: Compatible with 3.3.x (and above) agents **Workaround**: Re-enable SSLv3 until agents are upgraded. 1. Navigate to **Settings > Persistent Agent > Transport Configuration** 2. Under TLS Service Configuration panel, SSLv3 can be added in the TLS Protocols field.
8.3.x	For new installs and upgrades from older than 8.2, the "Default UDP" Persistent Agent Transport Configuration (UDP 4567) will initially be disabled. Agent versions 3.x and 4.x use both TCP 4568 and UDP 4567 to communicate. **Workaround**: After completing upgrade, re-enable the Default UDP Transport Configuration to allow FortiNAC to communicate to agents running pre-5.x versions. 1. In the Admin UI, navigate to **Settings > Persistent Agent > Transport Configuration**.

Version	Description
	2. Under **Packet Transport Configurations** panel, click **Add**. 3. Fill in the fields with the values below: **Name**: Default UDP **Bind to Address**: (leave blank) **Port**: 4567 **Maximum Incoming Packets to Queue**: 10000 **Transport Type**: UDP 4. To apply changes, click **Reload Services**

8.5.x and higher	Requires CentOS 7.4 or higher. The current CentOS version installed is listed as "Distribution" in the CLI login banner or typing "sysinfo".
	Example:
	`> sysinfo`
	`**********`
	`Recognized platform: Linux`
	`Distribution: CentOS Linux release 7.6.1810 (Core)`
	If the CentOS version is below 7.4, run OS updates and reboot before upgrading. For instructions on updating CentOS, refer to the Fortinet Document Library.
	A Network Access Policy is required for the user-id to be sent to the firewall for Palo Alto SSO and FortiGate RSSO integrations. For details, refer to related KB article FD49517.

8.8.x	Requires access to downloads.bradfordnetworks.com from each appliance or virtual machine. The update automatically installs CentOS files for the new Local Radius Server feature on the Control Server(s). If access is blocked, the software upgrade will fail. The default transfer protocol can be changed from FTP to either HTTPS or HTTP. For instructions, refer to the Appendix of the CentOS Updates reference manual. When upgrading from a pre-8.8 version to 8.8.0 or 8.8.1, the upgrade may hang if the appliance does not have external FTP access. The upgrade introduces a new local RADIUS server feature that requires additional CentOS patches. The download and installation of the patches occur during the upgrade process. A new .repo file is written in order to download the patches and specifies FTP as the transfer protocol. **Note:** As of 8.8.2, the default protocol was changed to HTTP. Customers that currently do not have a README and want to upgrade themselves should do the following: 1. Modify firewall to allow FTP access for the eth0 IP address for each appliance until upgrade is completed 2. Once completed, modify the repo files to the desired protocol for future OS updates. For instructions, see section Change Transfer Protocol to HTTP/HTTPS in the CentOS Updates document in the Fortinet Document Library. Customers that currently have a README, do not want to upgrade themselves, or cannot make the temporary firewall change should contact Support to schedule the upgrade. **802.1x implementations:** Port 1813 no longer listening after upgrading from pre-8.8 version. After upgrade, re-enable by performing the following steps: 1. Navigate to System > Settings > Authentication > Radius 2. Deselect Accounting Port 1813

Version	Description
	3. Click Save 4. Re-select Accounting Port 1813 5. Click Save See KB Article FD50889. https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD50889
8.8.3	• **Important:** Customers with 10.x XenMobile integrations must ensure XenMobile is running 10.10 or higher before upgrading FortiNAC. As of this version, FortiNAC no longer supports earlier 10.x XenMobile versions due to changes in API schema. This change does not affect 9.x versions of XenMobile. • Ensure http access is allowed to the internet for the FNAC eth0 IP address. This must be done for both Primary and Secondary servers in High Availability configurations. See KB FD51203.
8.8.5	• Functionality to register hosts using SNMP traps (LogOn Script) is disabled. After upgrading to 8.8.5 or later from a pre-8.8.5 version, re-enable the functionality. Contact Support for assistance. See KB FD51186. • Ensure http access is allowed to the internet for the FNAC eth0 IP address. This must be done for both Primary and Secondary servers in High Availability configurations. See KB FD51203.

Features No Longer Supported

Case #	Description
	Agent Server Communication: The InstallerEditor tool used to modify the server name in the Agent MSI files is no longer supported. It is recommended that you use DNS entries that can be used by the agent to look up the name of the FortiNAC server with which it should communicate. See Secure Agent Server Communications in the Help., Backup: Removed the ability to display or customize the list of files to be backed up on the Database Backup view.
	Bandwidth Management Plugin: The Bandwidth Management Plugin designed to log bandwidth usage on a per host basis has been removed from FortiNAC. The Bandwidth In and Out fields have been removed from the Top Users feature on the Connections View because they relied on the Bandwidth Management Plugin.
	Device Management: Device Management no longer supports Enterasys RBT wireless controllers.
31133	**Device Management**: Device Management no longer supports the HP WESM Chassis because this product is considered End of Life by HP.

Case #	Description
	Go Menu: The Go Menu has been replaced with a new menu bar structure across the top of the Admin UI. The option to enable this menu has been completely removed in Version 6.1.
40167	**LDAP Directory**: The field for "Distinguished Name (DN)" in the Group Attributes tab of the LDAP Settings will be removed in a future release. Support for treating users under an OU as a group will be removed in lieu of you creating directory groups.
	LDAP Directory: Support for Kerberos has been removed from the LDAP Directory Configuration as of V7.0.
29866	**Nessus Server**: The ability to add a Nessus Server in Topology View has been removed. Nessus Servers are no longer being supported.
00028024 00029418	**Operating Systems**: Clients with these Operating Systems are no longer supported: Windows 98 Windows Me Mac OS X 10.1, 10.2, 10.3. Mac OS X 10.5 is not supported for use with Agent Version 2.2.6 and higher.
	Packeteer/Packet Shaper/ Blue Coat: Support for integration with Packeteer Packet Shaper (now Blue Coat) has been removed.
	Plugins: The Scanning Engines plugin will be removed in a future release.
	Portal: Support for Portal v1 will be discontinued in the next major release (8.0). If you are still using portal v1 pages you should plan to transition to portal v2 before then.
	Reports: The default set of Crystal Reports has been removed from FortiNAC's Admin UI in FortiNAC version 8.0. This includes the Compliance Reports for Agent Versions, Guest Registrations By Date and Sponsor, Historical Scans, Host Registrations, Network Device Count, Network Devices By Device Type, Ports By VLAN, Registration Failures, Scans by Operating System, Scans by Policy and Users by Role. The capability to connect to FortiNAC's database with SAP Crystal Reports in order to produce your own reports will still be supported.
	Scan Scripts: The Security Plug-in designed to process user created scripts has been removed from the software.
	Windows 7 Edition Checking: Fortinet will not be providing validation of additional O/S editions for Windows 7. The current list of options (Home Basic, Home Premium, Professional, Enterprise, Enterprise N, Ultimate, Starter) will be all that are individually supported.

Upgrade Instructions

Upgrade Overview

This procedure describes how to update a FortiNAC appliance from the Admin UI. The Upgrade Considerations section above should be reviewed before proceeding.

For questions or concerns regarding upgrades, Assistance on page 13

Single Appliance or Appliance Pair (Control/Application Servers)

Upgrade System

See Upgrade Using the Administration UI.

After Upgrade

1. Exit and re-launch browser.
2. Run the Auto Definition Update Synchronization scheduled task to get the most recent definitions for Anti-Virus, Anti-Spyware and the valid vendor codes.
   a. Navigate to **System > Scheduler**
   b. Click **Auto-Definition Synchronizer**
   c. Click **Run Now**

High Availability Environments

The upgrade is performed on the Primary Server and automatically updates the Secondary Server(s).

If the Secondary Server(s) is in control, FortiNAC prevents you from updating and displays a message with detailed instructions indicating that the Primary must be running and in control.

Before upgrade
Verify all the appliances in the HA system are in the proper status:

- The Primary Server is running and in control.
- The Secondary Server(s) are running and not in control. This can be verified by viewing the Summary pane in the Dashboard of the Administration UI.

Upgrade System

Update the Primary server following the instructions for a regular system update. See Upgrade Using the Administration UI.

After Upgrade

1. Exit and re-launch browser
2. Re-save the High Availability configuration. This is required in order for the Primary Server to copy the license key to the Secondary Server. Otherwise, the function to fail over from Primary to Secondary Server will not work properly.
   Note: Management processes are automatically restarted upon saving the configuration.
   a. Navigate to **System > Settings > System Management > High Availability**
   b. Click **Save Settings**
3. Run the Auto Definition Update Synchronization scheduled task to get the most recent definitions for Anti-Virus, Anti-Spyware and the valid vendor codes.
   a. Navigate to **System > Scheduler**
   b. Click **Auto-Definition Synchronizer**
   c. Click **Run Now**

Network Control Manager Environments

When managing FortiNAC servers with a FortiNAC Control Manager, perform the update procedure from the Control Manager Admin UI.

Important: All managed servers must run the same version of code as the Control Manager.

Upgrade System

See Upgrade Using the Administration UI for instructions.

After Upgrade

1. Exit and re-launch browser.
2. On each set of managed appliances as well as the Manager, run the Auto Definition Update Synchronization scheduled task to get the most recent definitions for Anti-Virus, Anti-Spyware and the valid vendor codes.
   a. Navigate to **System > Scheduler**
   b. Click **Auto-Definition Synchronizer**
   c. Click **Run Now**

Upgrade Using the Administration UI

1. From the FortiNAC appliance Administration UI, go to **System > Settings**.
2. From the tree on the left side of the page, select the **Updates > System**.
3. Update the appropriate fields under the **System Update Settings** section to configure connection settings for the download server. Refer to the **System Update Settings** section in the applicable release notes for the appropriate values.
4. When the download settings have been entered, click **Save Settings**.
5. Click **Test** to verify connection to the downloads server.
6. If the test failed, enter the correct settings and try again.

7. Click the **Download** button. A dialog box displays a drop-down list of the available releases, named by version number.
8. Select the release you want to download, and click **Download** at the bottom of the window. A pop-up window displays the progress of the download, which may take a while.
9. Once the download is complete, return to the upgrade window.
10. If using a **FortiNAC Control Manager**, click the **Distribute** button to copy the update to all of the servers currently being managed by the FortiNAC Control Manager.
11. Start the upgrade by clicking the **Install** button.
12. On the Update dialog, select the version of the release you wish to install from the drop-down menu and then click **Update**. A pop-up window shows the progress of the update.
13. Verify that the correct version is now installed on the server by navigating to **Help > About** or via the CLI by typing "sysinfo". See Sysinfo Information Descriptions on page 12 for information regarding expected output.
14. Complete any further configurations required as per Upgrade Considerations section.

Sysinfo Information Descriptions

Sysinfo shows the following information:

Distribution: Lists the CentOS Operating System version and is updated via OS Update.

OS Kernel: Lists the OS update patch value. Note this will only change if a Kernel update is in the OS Update.

Engine Version: Lists the value of the system's Code Release. This is the version displayed in the Administration UI **Help > About** and is updated via product upgrade.

Firmware Version: This is the Image or OVA version and will not change.

Example

```
> sysinfo
************************************************************
Recognized platform: Linux
          Distribution: CentOS Linux release 7.6.1810 (Core)
             OS Kernel: 3.10.0-957.21.3.el7.x86_64
        Home directory: /root
         Terminal type: xterm


Product Type: NetworkControlApplicationServer
        Product Family: NetworkSentry
        Appliance Type: FortiNAC FNVMCA
        Engine Version: 8.6.2.587
            Build Date: Mon 25-Nov-2019
      Firmware Version: 8.6.0.320
         Firmware Date: 2019-07-29
************************************************************
```

Assistance

For license key installation issues, contact FortiNAC Support. For registration/license processing and all other issues, contact Fortinet Customer Service.

Contacting Customer Service and Support by Phone

USA +1 408 542 7780

Canada +1 613 670 8994

France +33 4 89 87 05 55

Malaysia +6 032 719 7601

Click the link below for a list of local toll-free telephone numbers to reach Fortinet:

http://www.fortinet.com/support/contact_support.html/

Online

https://support.fortinet.com/