FortiNAC - Upgrade OS and Software (CentOS)

Version F 7.2.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/training-certification

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

December 12, 2023
FortiNAC F 7.2.x Upgrade OS and Software (CentOS)
49-922-769106-20211216

TABLE OF CONTENTS

Overview

This document provides at-a-glance guidance on how to upgrade the Operating System (OS) and software of a FortiNAC appliance running CentOS.

Note: This cookbook does not apply to appliances running FortiNAC-OS operating system (FNC-CAX/FNC-MX).

Related documentation can be found in the "Release Information" Section of the Documentation Library (https://docs.fortinet.com/product/fortinac-f/7.2):

- CentOS Updates
  - Fortinet Update Policy and general requirements
  - Considerations
  - More detailed/comprehensive UI update instructions
  - CLI update instructions
  - Troubleshooting
- Upgrade Instructions and Considerations
  - Upgrade path requirements
  - Feature specific considerations
  - More detailed/comprehensive upgrade instructions
- Release Notes
  - Upgrade Requirements
  - Pre-Upgrade Procedures
  - New features
  - Enhancements and addressed issues
  - Known issues
  - Device support considerations
  - Added device support
  - System update settings
- Release Matrix – Listing of versions and their release date

Procedure Overview

1. Operating System Update: Update CentOS to ensure latest patches are applied
2. Product Version Update: Update FortiNAC Software
   Single or High Availability environment
   FortiNAC Manager environment

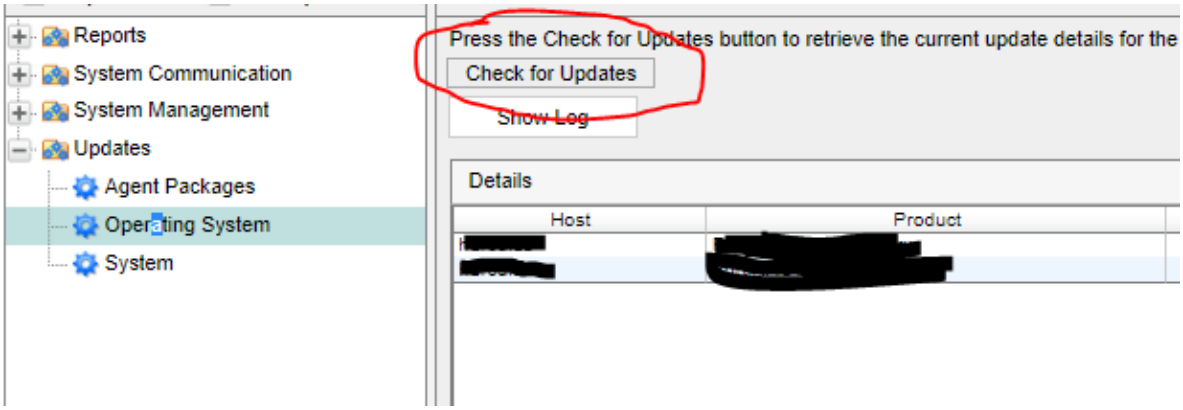
Step 1: OS Update

Prerequisites

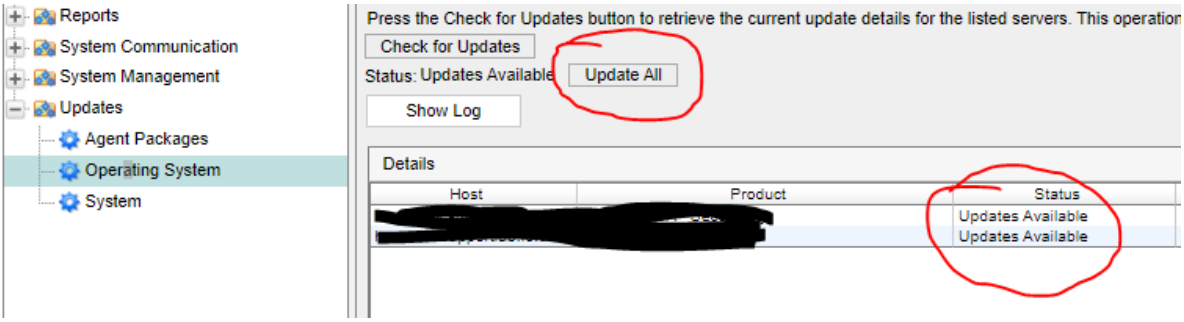
- All appliances will need access to the internet
- If virtual appliances, snapshots should be taken of all appliances

Procedure

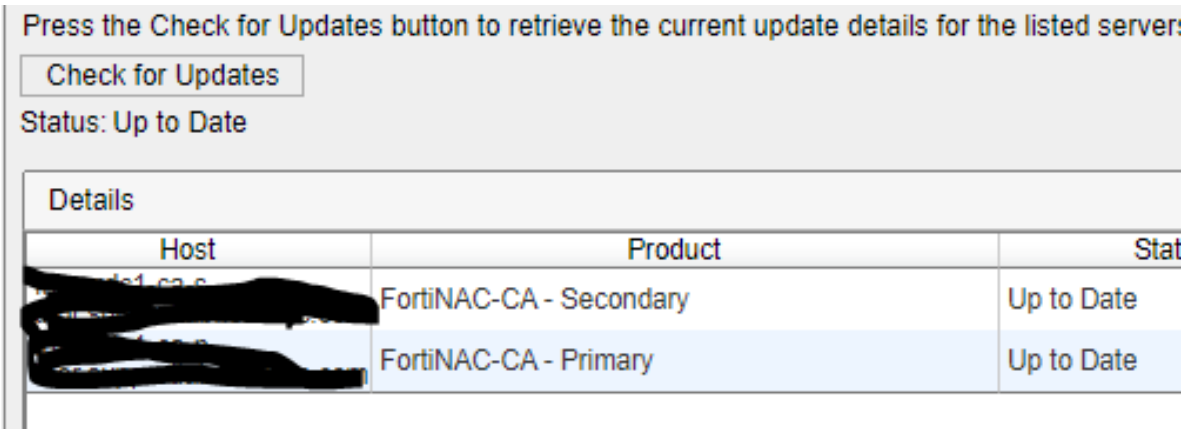
1. In the UI navigate to **System > Settings**.
2. Select **Updates,** then **Operating System**.
3. Select **Check for Updates** (this will take about a minute).



4. If updates are available, then you will see an option to Update All servers (this will take several minutes)



5. After about 3-4 minutes click on **Check for Updates.** Eventually it will return with Status of **Up to Date**.



6. Reboot ALL appliances. Navigate to **System > Settings**
7. Select **System Management,** then **Power Management**.
8. Reboot in this order but without delay:
   Secondary Server(s) (if High Availability configuration)
   Primary Application Server (if applicable)
   Primary Control Server or Primary Control/Application Server

Step 2: Product Version (Software) Update

Single and High Availability Environments

Prerequisites

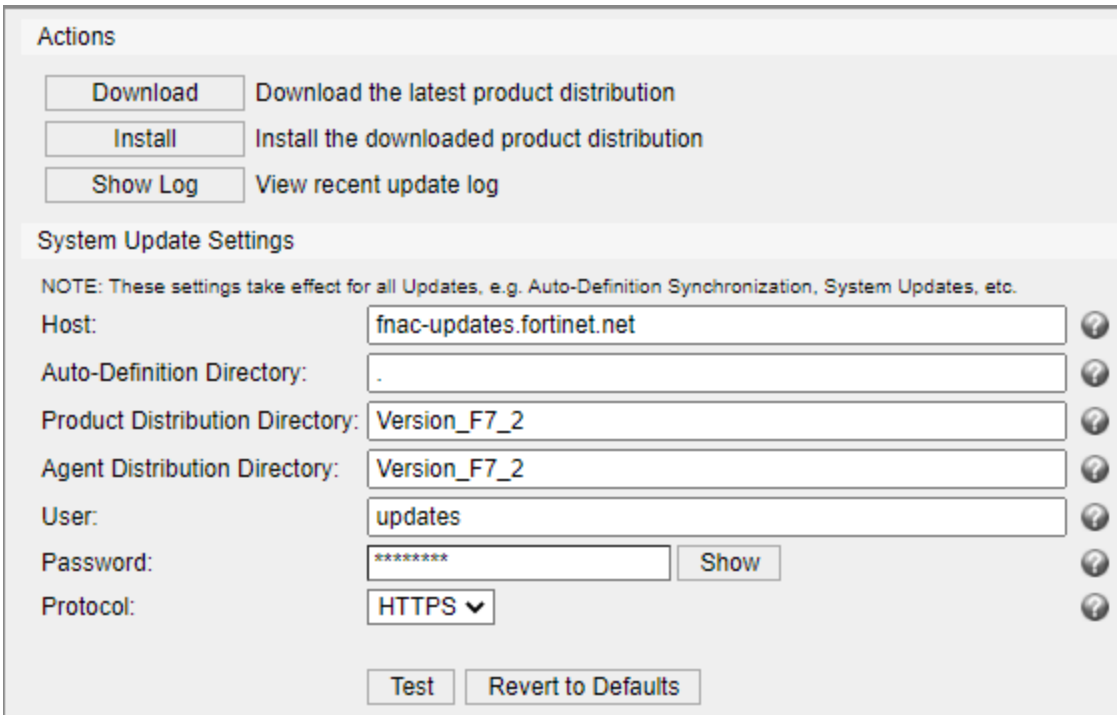
- **High Availability (FortiNAC versions 9.1.10, 9.2.8, 9.4.3, 7.2.2 and greater)**: In order to maintain communication between FortiNAC servers post-upgrade, a list of allowed serial numbers must be set. Customers can configure this list at any time prior to upgrade to avoid communication interruption. CLI access to each appliance is required. There is no service interruption when performing this change.
  For instructions, refer to the **Pre-Upgrade Procedures** section of the applicable Release Notes:
  F7.2.2 (CentOS)

Determine if upgrade can be done from UI:

1. Log in to CLI as root
2. Run this command
   `cat /bsc/campusMgrUpdates/README`
3. If there is no output or a line saying “No such file” proceed with the upgrade. If there is output, copy it and open a ticket to assist with the setup or the upgrade.

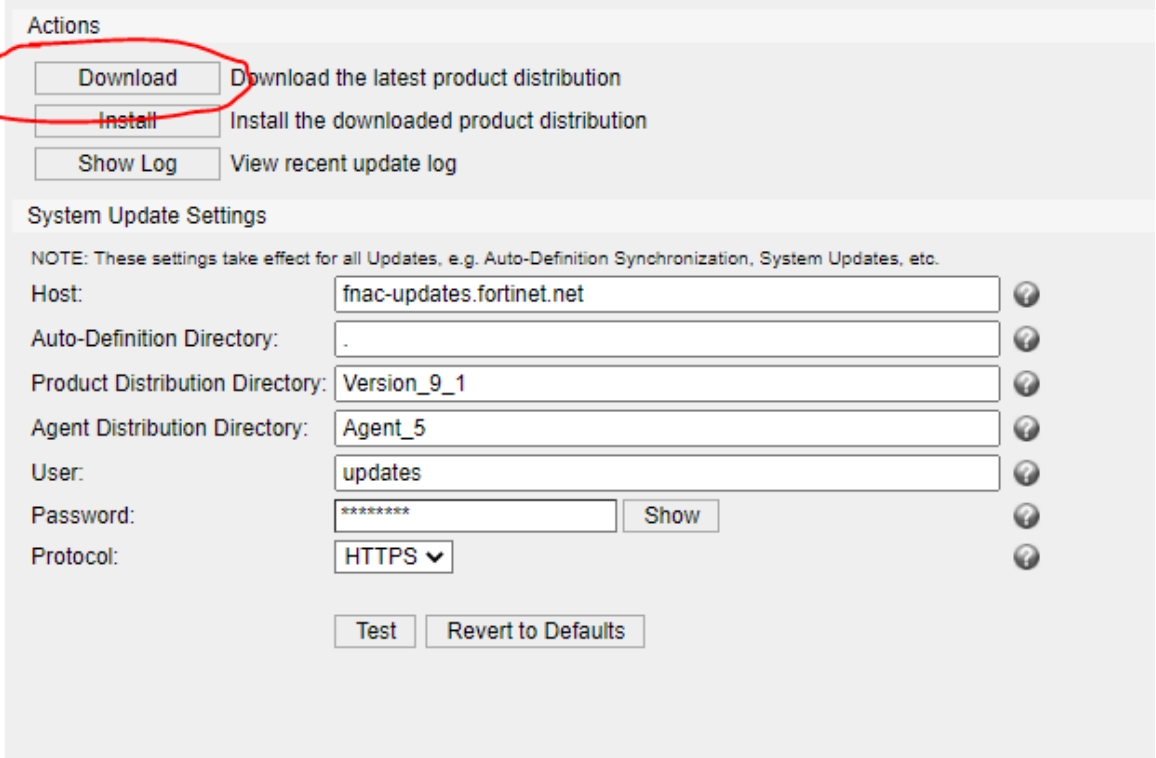
Procedure

1. In the UI navigate to **System →Settings**.
2. Select **Updates,** then **System**.
3. Confirm the information is correct based on the **System Update Settings** section of the Release Notes.

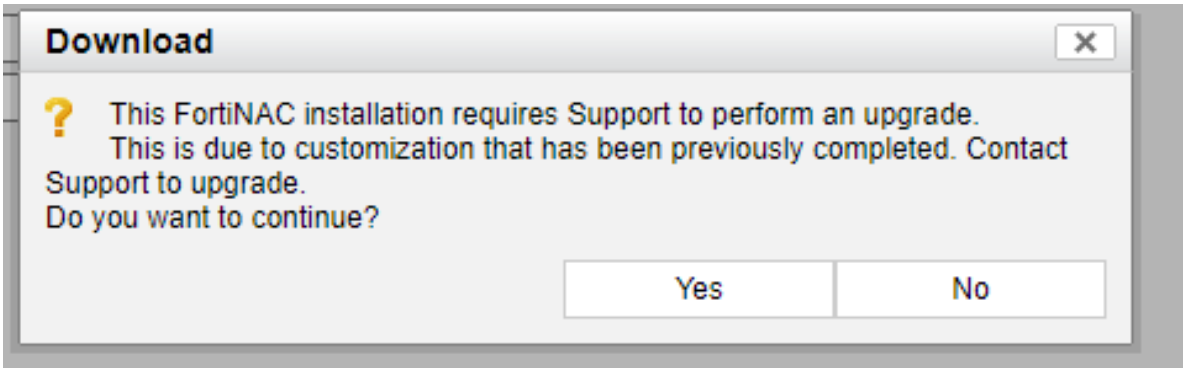
4. 

   All information is common except Product Distribution Directory. It is based on the following:

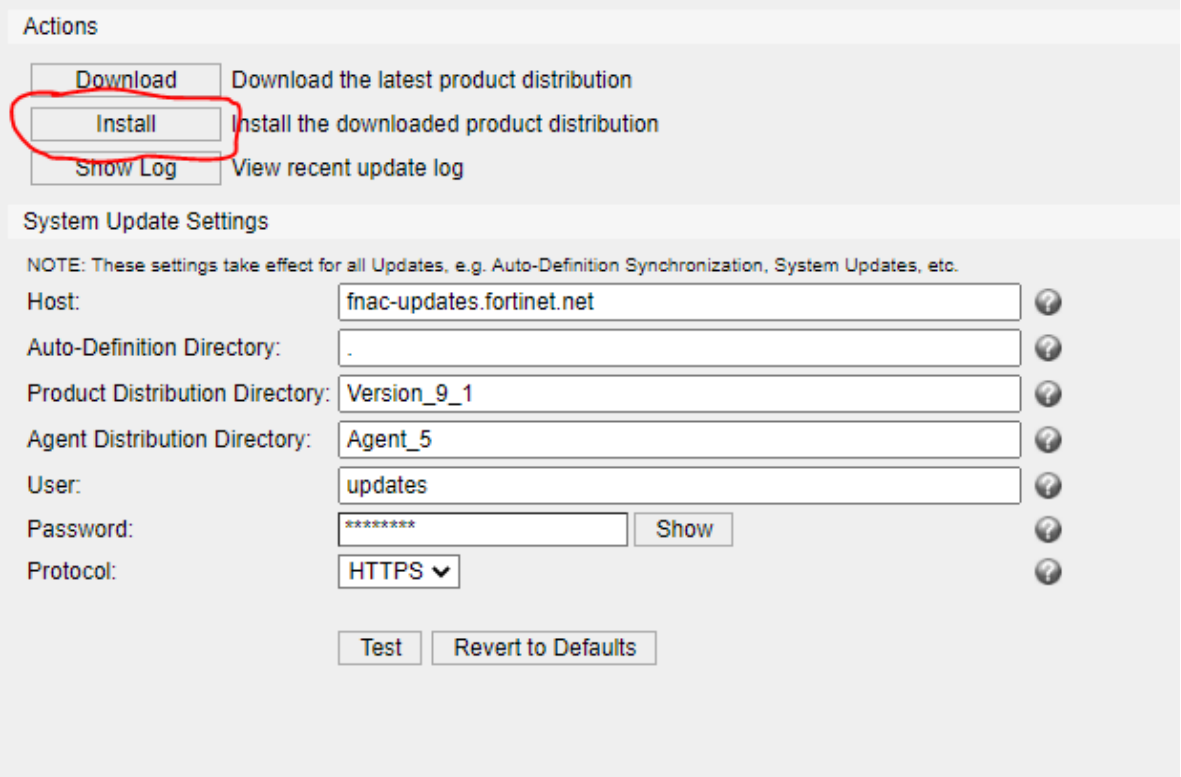
   Version F7.2x: Set to Version_F7_2
5. Save Setting.
6. Clicking **Test** should get a Success. If not, confirm settings above and the firewall allows https traffic from primary control server.
7. Download the Version that will be used to upgrade the system.



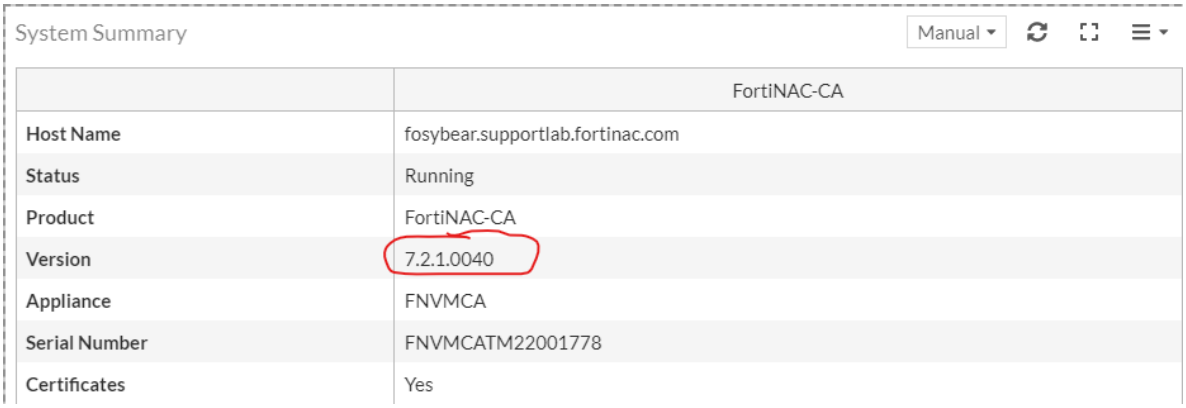
8. If the following error appears, refer to the Prerequisites. The code can still be downloaded, but the upgrade cannot be run via the UI.



9. Install/upgrade FortiNAC, this will take about 3-4 minutes and upgrades all appliances.



10. 10 Once it is done, the UI will show Processes Down. Close browser tab.
11. Clear the browser cache. Display anomalies may be experienced if this step is not done.
12. Wait about 2-3 minutes (may be longer for larger sites) then log back in.
13. Verify the new FortiNAC version is reflected.



	FortiNAC-CA
Host Name	fosybear.supportlab.fortinac.com
Status	Running
Product	FortiNAC-CA
Version	7.2.1.0040
Appliance	FNVMCA
Serial Number	FNVMCATM22001778
Certificates	Yes

14. 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 is complete. Contact Support for assistance.

Troubleshooting

Upgrade aborts when remote backup fails

Upgrade fails with license requirement error

'Licensed without certificates' message in UI

Certificates not included in license keys

FortiNAC Manager Environments

In environments where there is a FortiNAC Manager and multiple FortiNAC systems, the option is available to perform the upgrade for all systems from the Manager.

Prerequisites

- Appliances will need access to the internet
  - Option 1: Upgrade via Manager: Only FortiNAC Manager needs access
  - Option 2: Upgrade individually: The following will require access
    - FortiNAC Manager
    - Single appliances
    - Primary Server in High Availability pairs
- If virtual appliances, snapshots should be taken of all appliances
- **FortiNAC versions 7.2.2 and greater**: In order to maintain communication between Manager and the managed systems post-upgrade, a list of allowed serial numbers must be set. Customers can configure this list at any time prior to upgrade to avoid communication interruption. CLI access to each appliance is required. There is no service interruption when performing this change.

  For instructions, refer to the **Pre-Upgrade Procedures** section of the applicable Release Notes:

  F7.2.2 (CentOS)
- **Managed Servers**: If the below requirements are not met, the update must be run from the managed server's Administration UI and not the Manager.
  - Must use the same Operating System (CentOS or FortiNAC-OS) as the Manager.

    Example:

    FNC-M-xx (CentOS) can upgrade FNC-CA-xx (CentOS)

    FNC-MX-xx (FortiNAC-OS) can upgrade FNC-CAX-xx (FortiNAC-OS)

    FNC-MX-xx (FortiNAC-OS) *cannot* upgrade FNC-CA-xx (CentOS)
  - Managers using FortiNAC-OS (FNC-MX-xx) can only update managed servers running on the same virtual appliance platform.

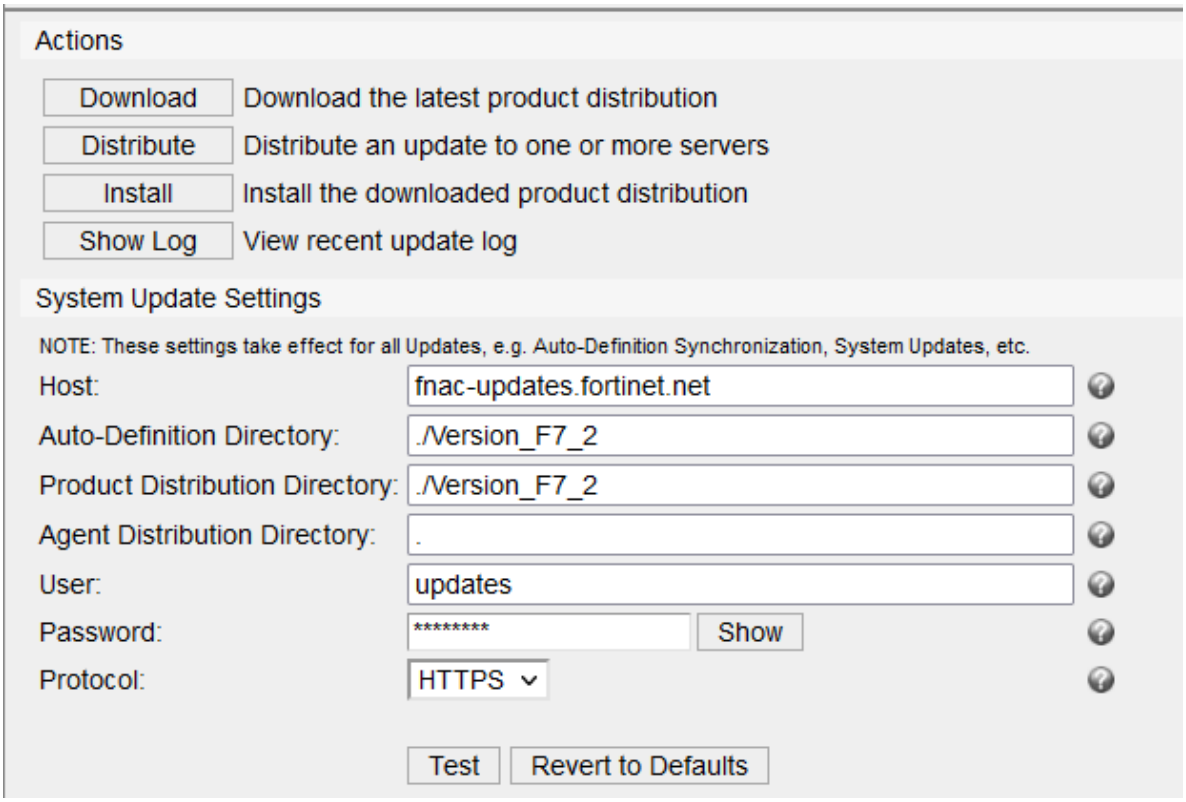
    Example:

    FNC-MX-xx on VMware can upgrade FNC-CAX-xx on VMware

    FNC-MX-xx on VMware *cannot* upgrade FNC-CAX-xx on Hyper-V

Procedure

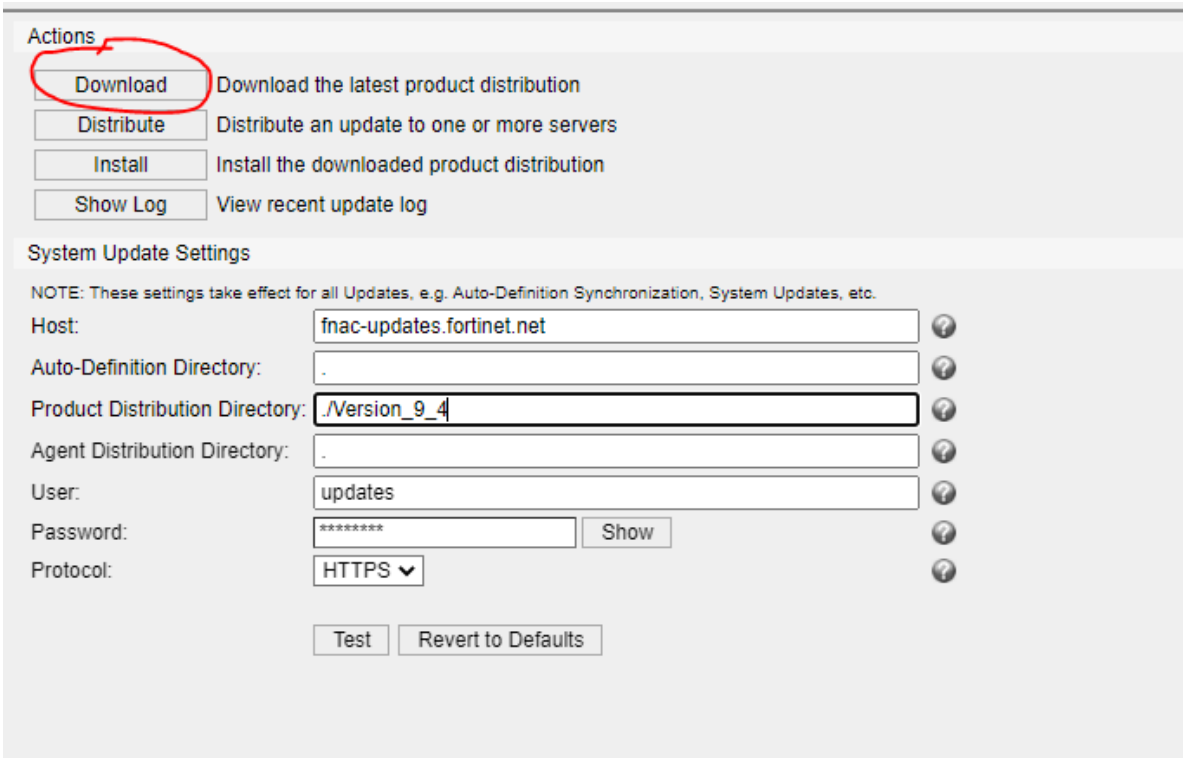
1. In the UI of the FortiNAC Manager, navigate to **System →Settings**.
2. Select **Updates,** then **System**.
3. Confirm the information is correct.



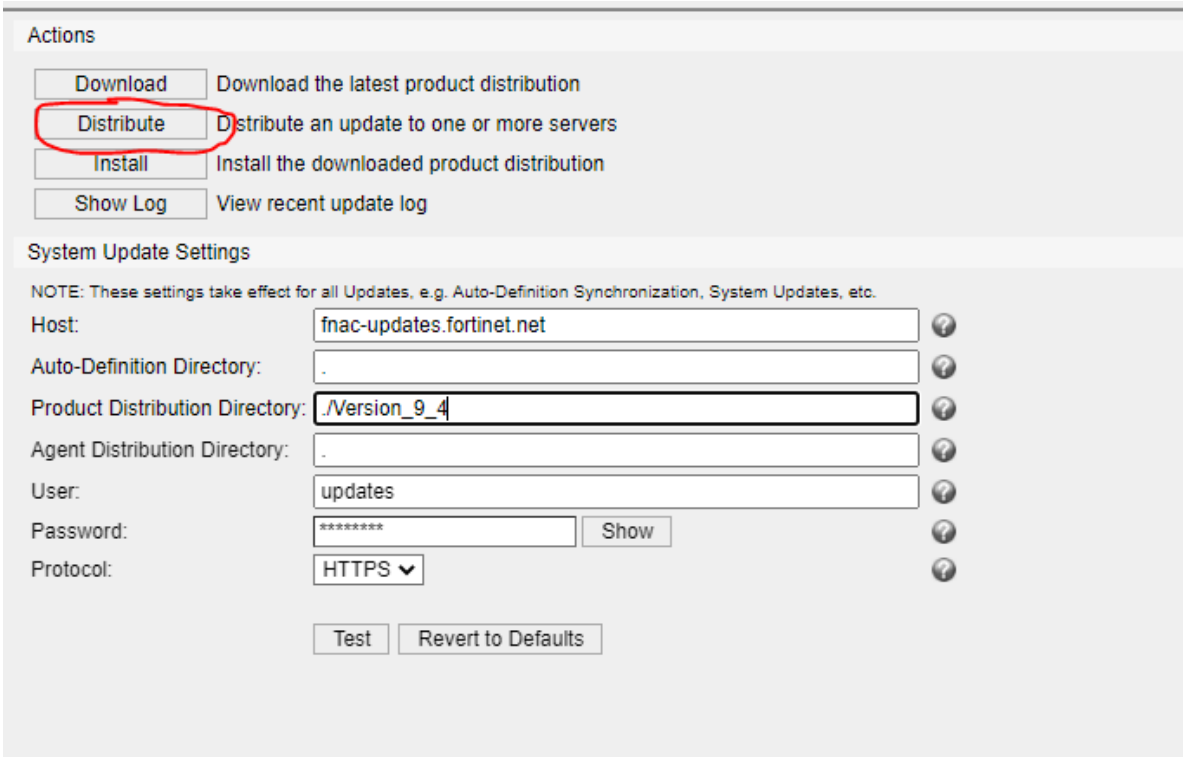
All information is common except Product Distribution Directory. It is based on the following:

Version F7.2x: Set to Version_F7_2

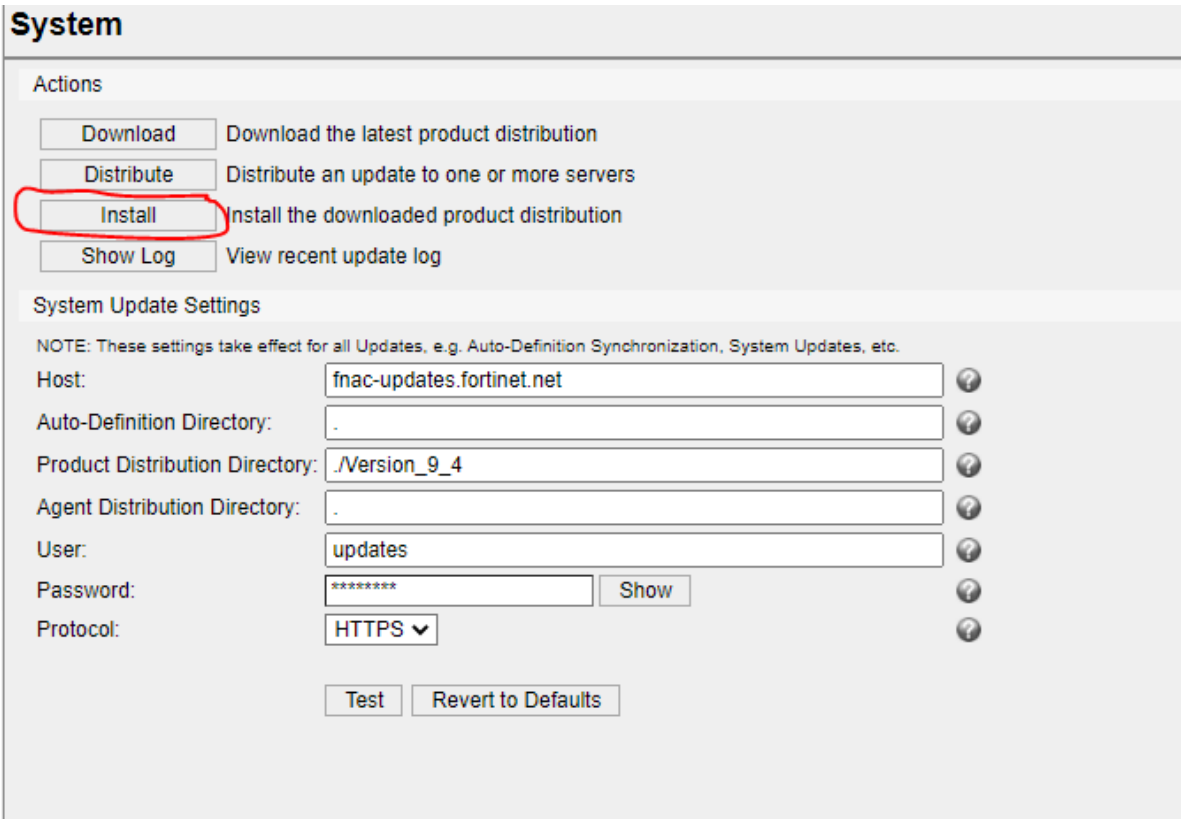
4. Save Setting.
5. Clicking **Test** should get a Success. If not, confirm settings above and the firewall allows https traffic from primary control server.
6. **Download** the Version for the upgrade.



7. Once downloaded, **Distribute** to all servers.



8. Once distributed to all systems, **Install** the new Version.



Upon clicking **Install**, the managed systems upgrade first, followed by the Manager.

9. Towards the end of the upgrade process, the UI will show Processes Down. Close browser tab.
10. Clear the browser cache. Display anomalies may be experienced if this step is not done.
11. Close browser tab. Wait about 2-3 minutes (may be longer for larger sites) then log back in.
12. Verify the new FortiNAC version is reflected in the **System Summary** Dashboard Widget of the appliance.

13. In each appliance UI, 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**.
14. Confirm all servers are listed in **Servers** Dashboard Widget of the Manager UI. Status should show **Running**.

Troubleshooting

Upgrade aborts when remote backup fails