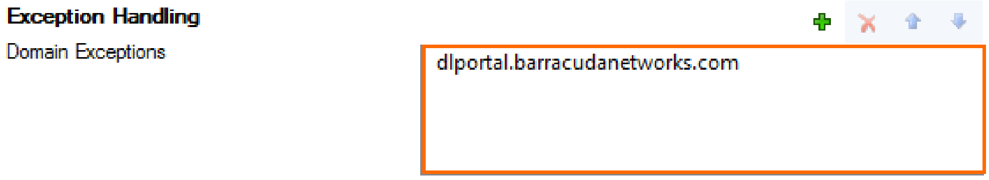
How to Update Control Center Managed F-Series Firewalls

The NextGen Control Center can manage multiple clusters, each using different firmware versions. The Control Center can only manage F-Series Firewalls of the firmware the Control Center is running. This means it is not possible to configure 7.0. features using a Control Center running an older firmware. You cannot mix different firmware versions in a cluster. When upgrading your firmware, update the Control Center first, then all managed firewalls, virtual servers, and services in the cluster. After all managed firewalls in a cluster have been updated, you must also migrate the cluster to the new release version. The Control Center checks every hour if new updates are available for the cluster versions that are configured. This also means that when a new cluster with a previously unused cluster version is created in the Control Center, it may take up to one hour for the corresponding updates, hotfixes, and patches to be displayed.

Before you begin

If you are using SSL Interception on your border firewall, you must add **dlportal.barracudanetworks.com** to the SSL Interception **Domain Exceptions** on the ***your F-Series Firewall*** **> Virtual Servers > Assigned Services > Firewall > Security Policy** page.



Exception Handling

Domain Exceptions: dlportal.barracudanetworks.com

Step 1: Verify the compatibility of the Control Center firmware with the managed firewalls

The following table shows compatibility between the major versions of the Control Center and various systems. Upgrade the Control Center to the same, or newer, firmware version before updating the managed Firewalls.

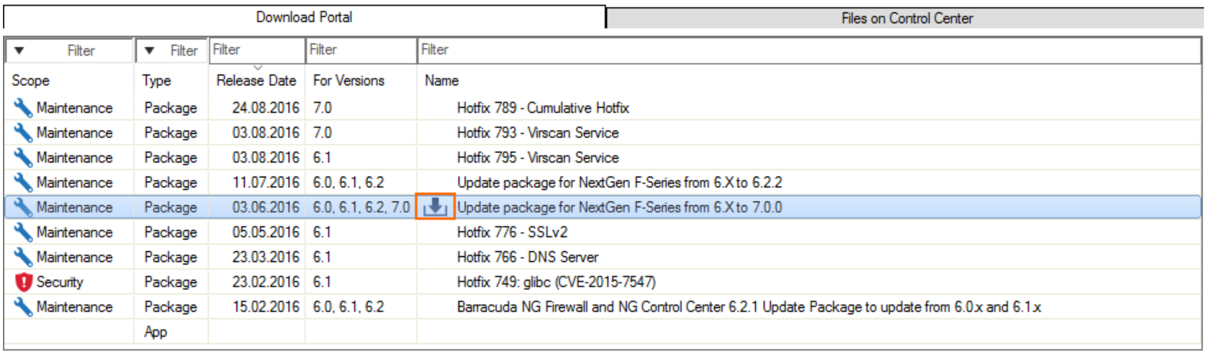
For more information, see Updating F-Series Firewalls and Control Centers

Step 2. Download the update package to the Control Center

Download the update package to the Control Center.

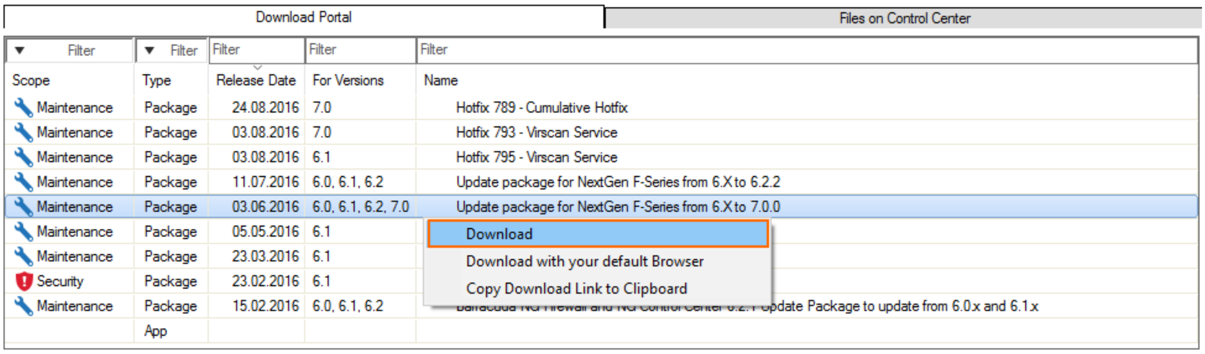
Do not use SSL Interception for the connection to the Barracuda Download Portal.

1. Log into the Control Center.
2. Go to **CONTROL > Firmware Update**.
3. In the lower half of the screen, click on the **Download Portal** tab.
4. Move the mouse over the desired update package. The download icon is displayed.



Scope	Type	Release Date	For Versions	Name
Maintenance	Package	24.08.2016	7.0	Hotfix 789 - Cumulative Hotfix
Maintenance	Package	03.08.2016	7.0	Hotfix 793 - Virscan Service
Maintenance	Package	03.08.2016	6.1	Hotfix 795 - Virscan Service
Maintenance	Package	11.07.2016	6.0, 6.1, 6.2	Update package for NextGen F-Series from 6.X to 6.2.2
Maintenance	Package	03.06.2016	6.0, 6.1, 6.2, 7.0	Update package for NextGen F-Series from 6.X to 7.0.0
Maintenance	Package	05.05.2016	6.1	Hotfix 776 - SSLv2
Maintenance	Package	23.03.2016	6.1	Hotfix 766 - DNS Server
Security	Package	23.02.2016	6.1	Hotfix 749: glibc (CVE-2015-7547)
Maintenance	Package	15.02.2016	6.0, 6.1, 6.2	Barracuda NG Firewall and NG Control Center 6.2.1 Update Package to update from 6.0.x and 6.1.x
	App			

5. Click the download icon, and select **Download**.

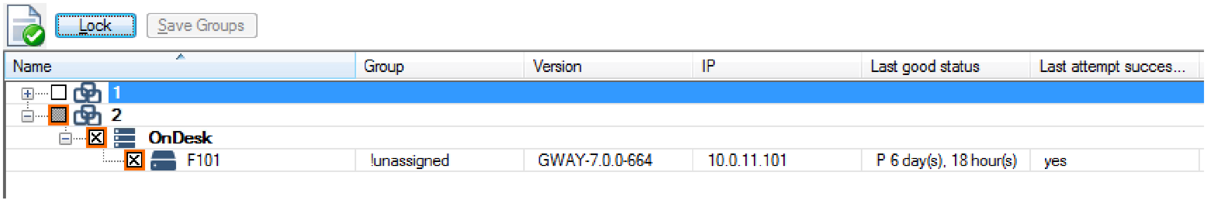


Scope	Type	Release Date	For Versions	Name
Maintenance	Package	24.08.2016	7.0	Hotfix 789 - Cumulative Hotfix
Maintenance	Package	03.08.2016	7.0	Hotfix 793 - Virscan Service
Maintenance	Package	03.08.2016	6.1	Hotfix 795 - Virscan Service
Maintenance	Package	11.07.2016	6.0, 6.1, 6.2	Update package for NextGen F-Series from 6.X to 6.2.2
Maintenance	Package	03.06.2016	6.0, 6.1, 6.2, 7.0	Update package for NextGen F-Series from 6.X to 7.0.0
Maintenance	Package	05.05.2016	6.1	
Maintenance	Package	23.03.2016	6.1	
Security	Package	23.02.2016	6.1	
Maintenance	Package	15.02.2016	6.0, 6.1, 6.2	Barracuda NG Firewall and NG Control Center 6.2.1 Update Package to update from 6.0.x and 6.1.x
	App			

After the download finishes, the update package is available in the **Files on Control Center** tab.

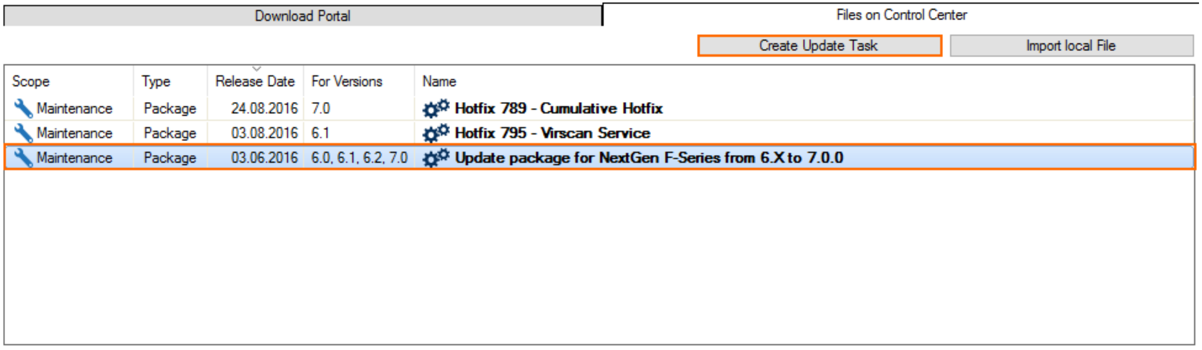
Step 3. Send the update package to the managed firewalls

1. On the **Firmware Update** page, select the ranges, clusters, and/or individual Firewalls to be updated.



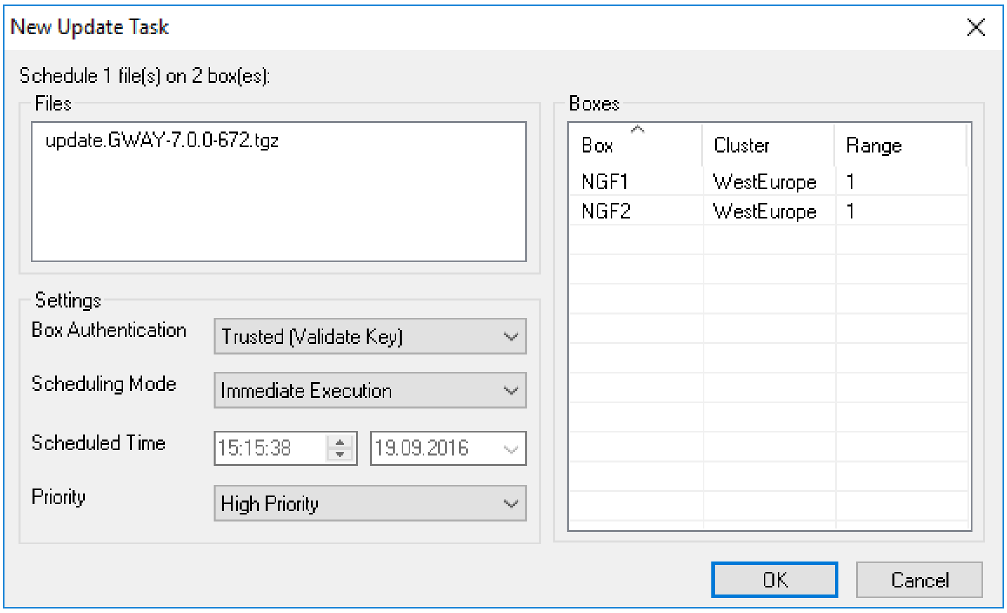
Name	Group	Version	IP	Last good status	Last attempt succes...
□ 1					
▨ 2					
☒ OnDesk					
☒ F101	!unassigned	GWAY-7.0.0-664	10.0.11.101	P 6 day(s), 18 hour(s)	yes

2. In the **Files on Control Center** tab, select the update package.
3. Click **Create Update Task**. The **New Update Task** window opens.



Scope	Type	Release Date	For Versions	Name
Maintenance	Package	24.08.2016	7.0	**Hotfix 789 - Cumulative Hotfix**
Maintenance	Package	03.08.2016	6.1	**Hotfix 795 - Virscan Service**
Maintenance	Package	03.06.2016	6.0, 6.1, 6.2, 7.0	**Update package for NextGen F-Series from 6.X to 7.0.0**

4. (optional) Select the **Scheduling Mode**.



New Update Task

Schedule 1 file(s) on 2 box(es):

Files

update.GWAY-7.0.0-672.tgz

Settings

Box Authentication: Trusted (Validate Key)

Scheduling Mode: Immediate Execution

Scheduled Time: 15:15:38 19.09.2016

Priority: High Priority

Boxes

Box	Cluster	Range
NGF1	WestEurope	1
NGF2	WestEurope	1

5. Click **OK**.

The update packages are now copied to the selected remote systems. Go to **CONTROL > Update Tasks** for more information.

Step 4. Execute the update package

1. Go to **CONTROL > Update Tasks**.
2. In the ∑ column, a green icon is displayed, verifying that the update package was sent successfully.
3. Select the systems that have received the entire update package and right-click the system select **Perform Update**.
4. In the **Schedule Task** window, select **Immediate Execution** from the **Scheduling Mode** list and click **OK**.

Wait for the update to finish. Depending on the system hardware, the process can last anywhere from 15 minutes (for a fast system) to 60 minutes (for flash appliances).

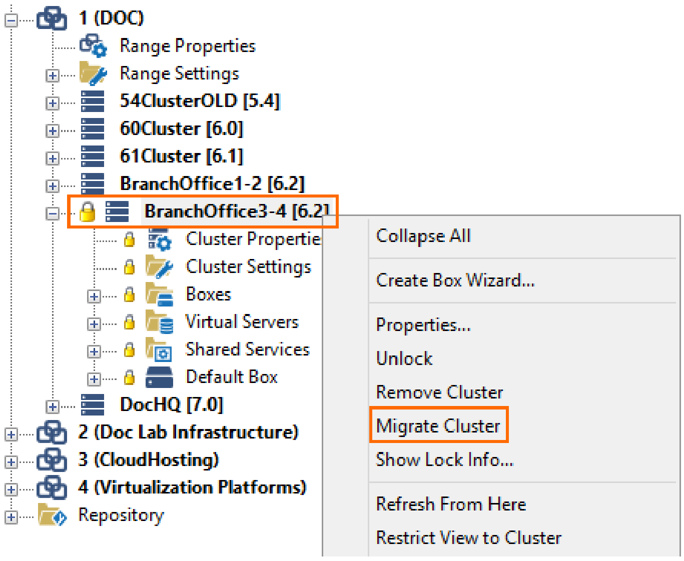
Unless otherwise noted, NextGen F-Series Firewalls will reboot after the update has been applied.

Step 5. Migrate the configuration version of the cluster

If you are updating to a new major version (5.4. to 6.0, 6.0 to 6.1, 6.1 to 6.2, or 6.2 to 7.0), you must migrate the cluster version after the update has completed.

Update the clusters individually

1. Open the cluster you just updated (**CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster***).
2. Right-click on the cluster and select **Lock**.
3. Right-click on the cluster and select **Migrate Cluster**.



4. Select the new **Release** version.
5. Click **OK**.
6. Click **Activate**.

Update all clusters in a range

If all clusters in the range are on the same firmware version, you can migrate all clusters simultaneously.

1. Open the range containing the clusters you just updated (**CONFIGURATION > Configuration Tree > Multi-Range >** ***your range***).
2. Right-click on the range and select **Lock**.
3. Right-click on the range and select **Migrate Range**.
4. Select the new **Release** version.
5. Click **OK**.
6. Click **Activate**.

Troubleshooting / logs

After the update process, review the **Box\Release\update** or **Box\Release\update_hotfix** log for each system to verify that it was successfully updated. To view a system log, you must connect directly to the firewall and open the **Logs** page.

Figures