How to Update Control Center-Managed CloudGen Firewalls

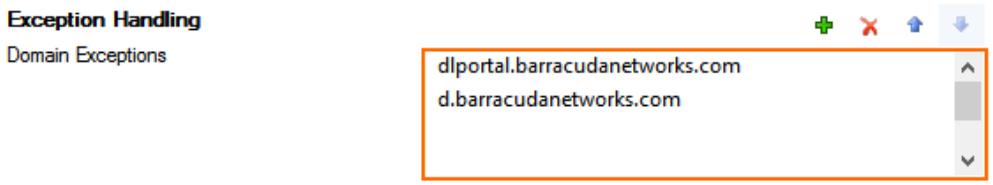
https://campus.barracuda.com/doc/79463148/

A Control Center can manage multiple clusters with each cluster using a different firmware version. However, the Control Center can only manage firewalls running the same or older firmware versions as the firmware version of the Control Center. Therefore, you cannot configure 7.2.0 features with a Control Center that is running firmware older than 7.2.0. It is also not possible to mix different major firmware versions in a cluster. If required, update your Control Center before updating your managed firewalls to a newer firmware version. After major version updates, the cluster version on the Control Center must be migrated to match the new firmware version.

The Control Center checks every hour for updates relevant to the configured cluster versions. It can take up to one hour for the updates, hotfixes, and patches to be displayed when a new cluster with a previously unused cluster version is created.

Before You Begin

If you are using SSL Inspection on your border firewall, you must add **dlportal.barracudanetworks.com** and **d.barracudanetworks.com** to the SSL Inspection **Domain Exceptions** on the ***your CloudGen Firewall*** **> Assigned Services > Firewall > Security Policy** page. To use SSL Inspection the **Feature Level** of the Forwarding Firewall must be set to **7.2** or higher. For more information, see SSL Inspection in the Firewall .



Step 1: Verify the Compatibility of the Control Center Firmware with the Managed Firewalls

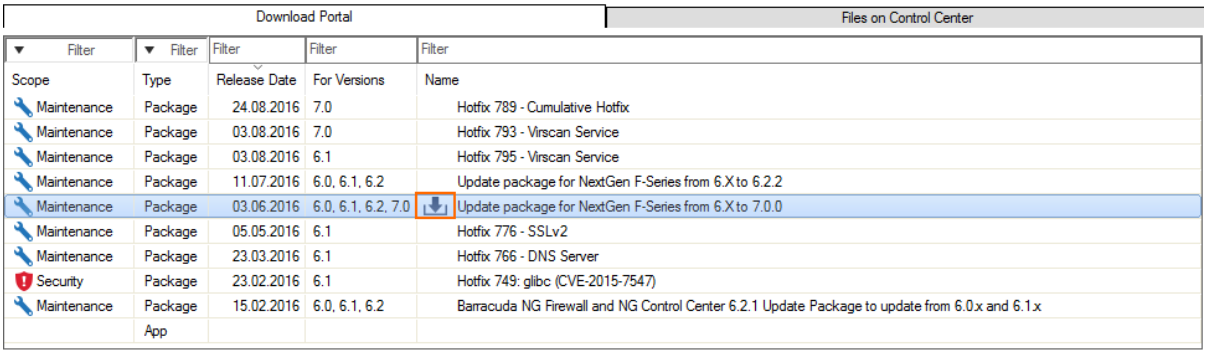
Before updating a managed firewall to a higher firmware version, verify that the Control Center is running a firmware version that is equal to or higher than the highest firmware version used by a managed firewall after the update.

For more information, see Updating CloudGen Firewalls and Control Centers.

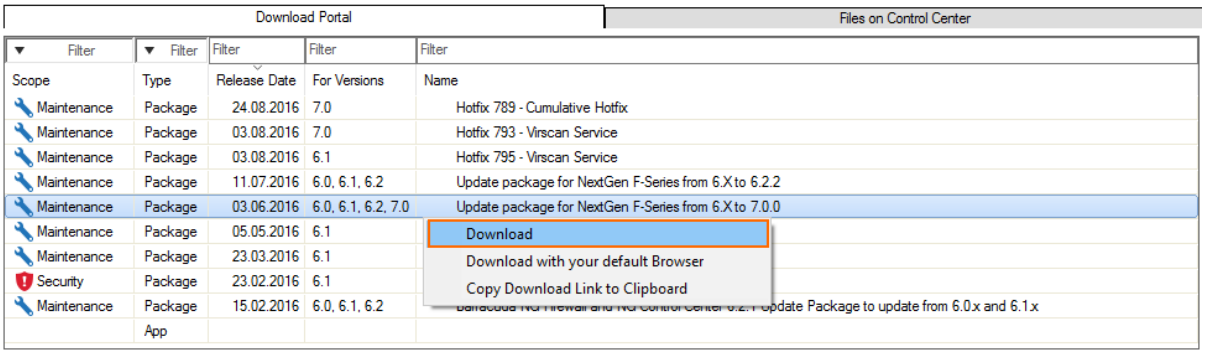
Step 2. Download the Update Package to the Control Center

Download the update package to the Control Center.

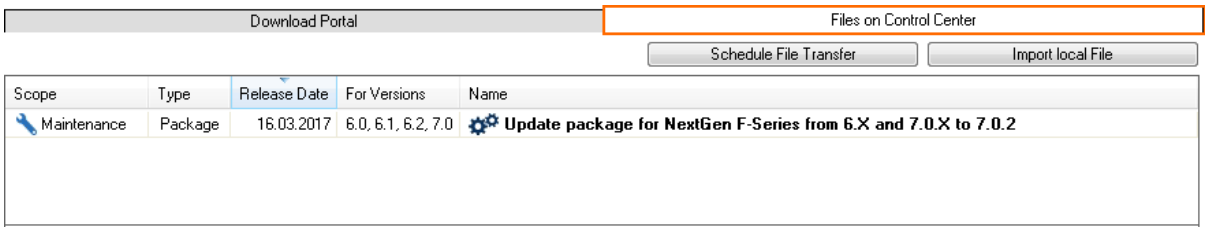
1. Log into the Control Center.
2. Go to **CONTROL > Firmware Update**.
3. In the lower half of the screen, click the **Download Portal** tab.
4. Move the mouse over the desired update package to display the download icon.



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

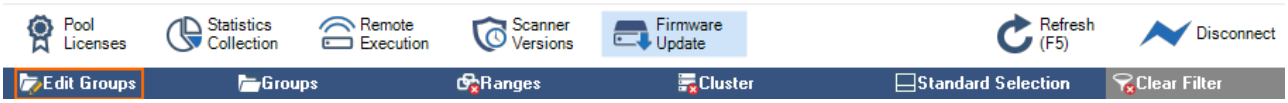


After the download finishes, the update package is available in the **Files on Control Center** tab.

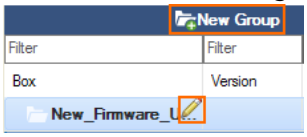


Step 3. (optional) Create Update Groups

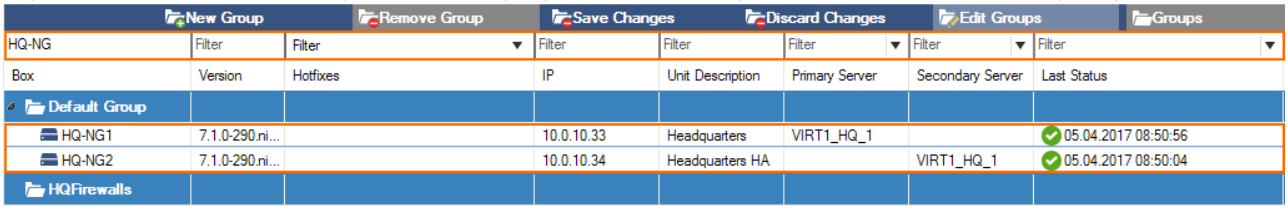
1. Go to **CONTROL > Firmware Update**.
2. In the ribbon bar, click **Edit Groups**.



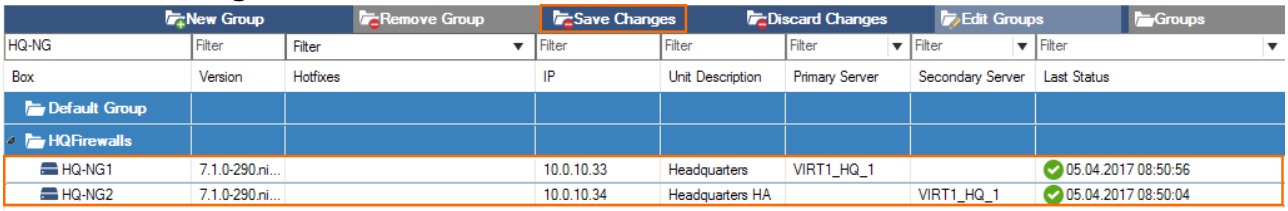
3. Click **New Group**. A new update group is created in the list.
4. Hover over the new group and click the edit icon.



5. Enter a name for the update group.
6. (optional) Use the Filter options to display the firewalls you want to add to this group.

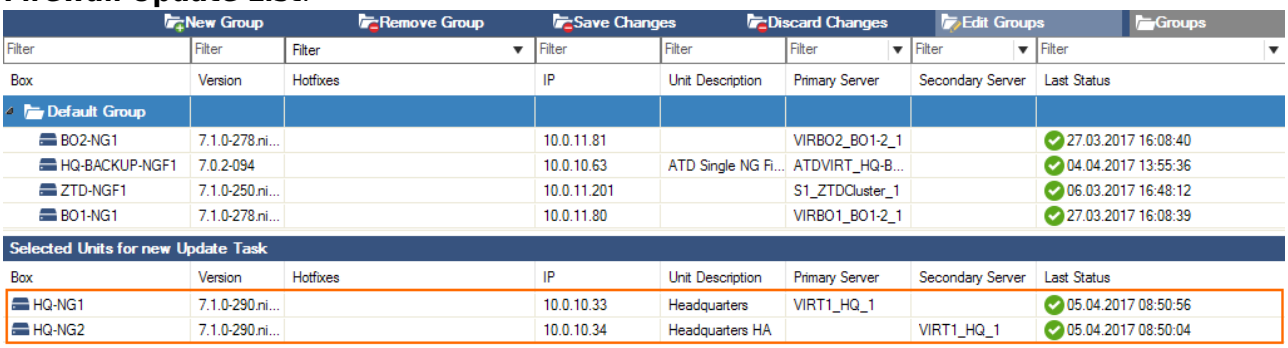


7. Select, then drag and drop firewalls to the new user group.
8. Click **Save Changes**.

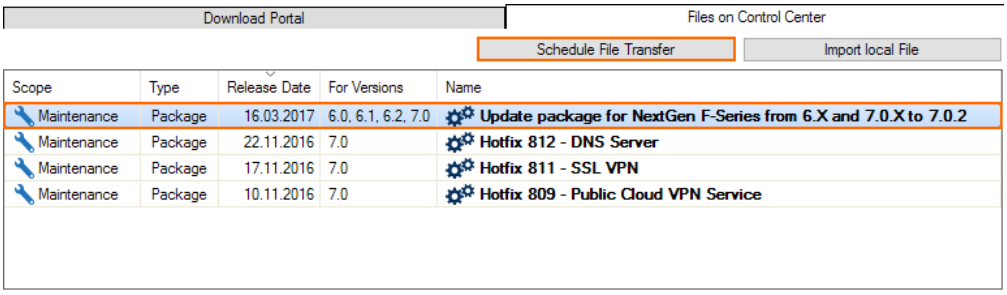


Step 3. Schedule the Firmware Update File Transfer

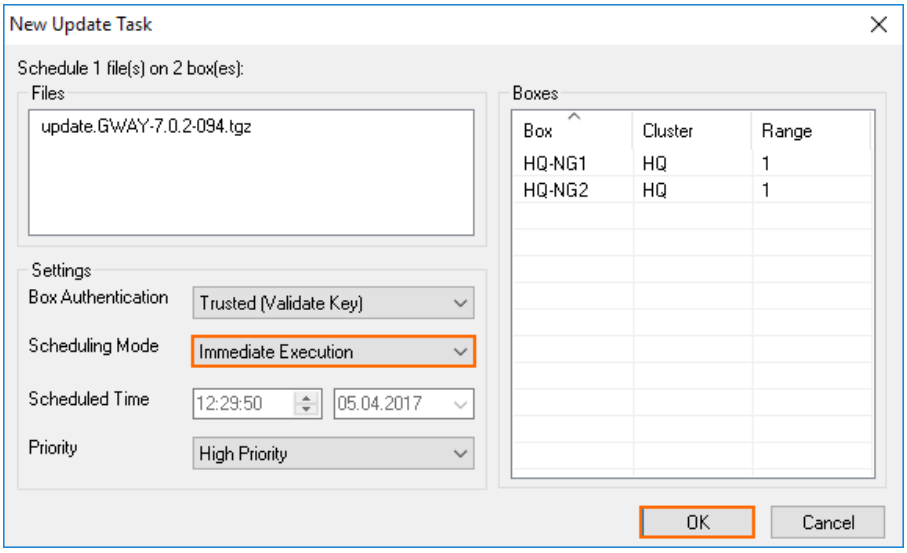
1. Go to **CONTROL > Firmware Update**.
2. Double-click each firewall and/or update group. The firewalls are added to the **Selected Firewall Update List**.



3. In the **Files on Control Center** tab, select the update package.
4. Click **Schedule File Transfer**. The **New Update Task** window opens.



5. (optional) Select the **Scheduling Mode** and **Schedule Time** to schedule a time for the file transfer.

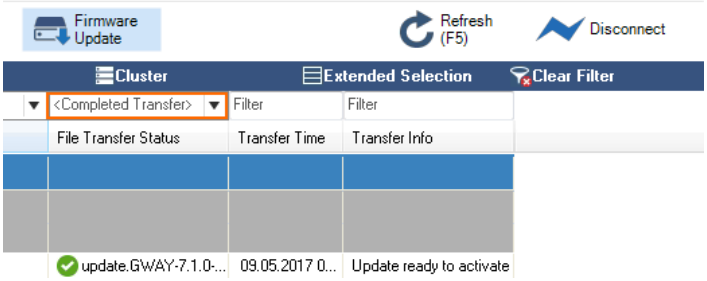


6. Click **OK**.

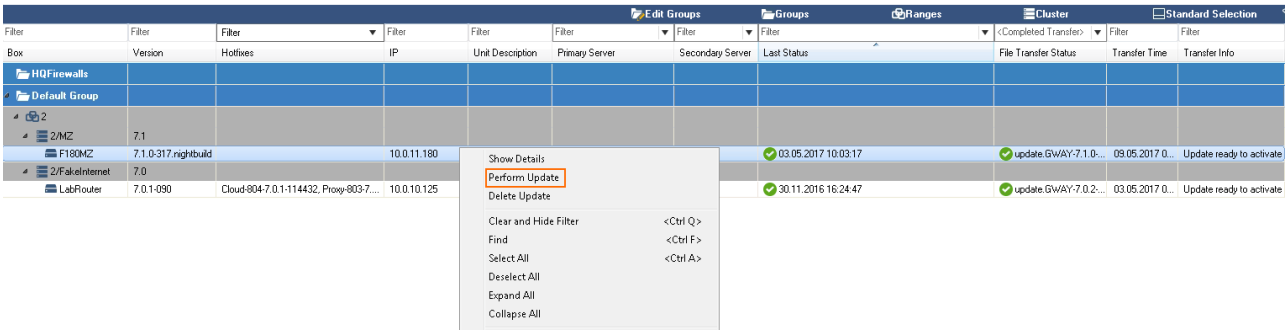
The update packages are now copied to the selected remote systems.

Step 4. Execute the Update Package

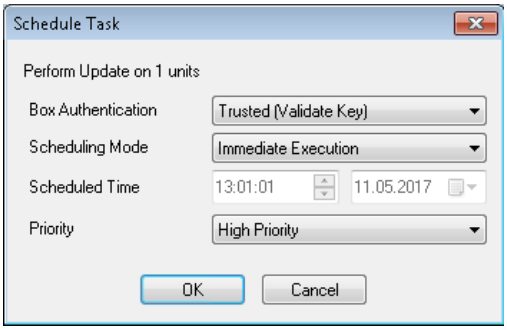
1. Go to **CONTROL > Firmware Update**.
2. In the **File Transfer Status** column, select **Completed Transfer**. The list of firewalls with completed transfers is displayed.



3. Select the firewalls to perform the update. Select multiple firewalls by holding down the CTRL (Strg) key.
4. Right-click the selected firewalls and click **Perform Update**. The **Schedule Task** window opens.



5. (optional) Configure the time and authentication settings for the update:
   - **Box Authentication** – Select **Trusted (Validate Key)**.
   - **Scheduling Mode** – Select **Immediate Execution** to update immediately, or **Delayed Execution** to set the time the update is triggered
   - **Priority** – When multiple tasks are configured for execution, the priority setting determines the execution order.



6. 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).

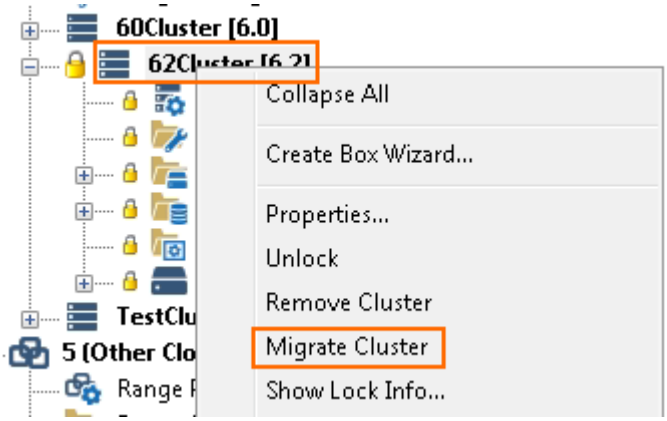
Unless otherwise noted, the appliance will reboot after the update.

Step 5. Migrate the Configuration Version of the Cluster

If you are updating to a new major version (e.g., 6.0 to 6.2, or 6.2 to 7.1), migrate the cluster version to the new major version after the update has completed. Multiple migrations may be required to reach the cluster version matching the firmware version.

Update the Clusters Individually

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster*** .
2. Right-click the cluster and select **Lock**.
3. Right-click the cluster and select **Migrate Cluster**.

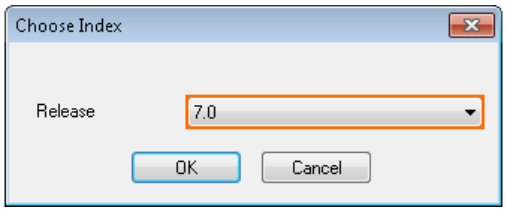


4. Select the new **Release** version.
5. Click **OK**.
6. Click **Activate**.

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. Go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range*** .
2. Right-click the range and select **Lock**.
3. Right-click the range and select **Migrate Range**.
4. Select the new **Release** version.
5. Click **OK**.



6. Click **Activate**.

Migrating the cluster version may have to be done multiple times if the firmware update skipped major firmware versions. E.g., When updating from 6.0 to 7.0.

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 go to the **Logs** tab.

Figures

1. fw_update00.png
2. cc_update_element_01.png
3. cc_update_element_02.png
4. cc_update_element_03.png
5. fwupdate_groups_01.png
6. fwupdate_groups_02.png
7. fwupdate_groups_03.png
8. fwupdate_groups_04.png
9. managed_updates_01.png
10. managed_updates_02.png
11. managed_updates_03.png
12. managed_updates_04.png
13. managed_updates_05.png
14. managed_updates_06.png
15. managed_updates_07.png
16. managed_updates_08.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.