

Secure Connector Firmware Update

<https://campus.barracuda.com/doc/79462665/>

The Control Center manages the distribution and update process for Secure Connector firmware updates. The admin must first update the firmware package to the Control Center and select the Secure Connectors from the list. The Control Center then distributes the file. Afterwards, the admin can trigger the update process and monitor the progress of the update.

Step 1. Verify the Compatibility of the Secure Connector with the Control Center Firmware

Verify that the Control Center firmware version supports the target Secure Connector firmware version. If necessary upgrade the Control Center before updating the managed Secure Connectors.

For more information, see [Updating CloudGen Firewalls and Control Centers](#).

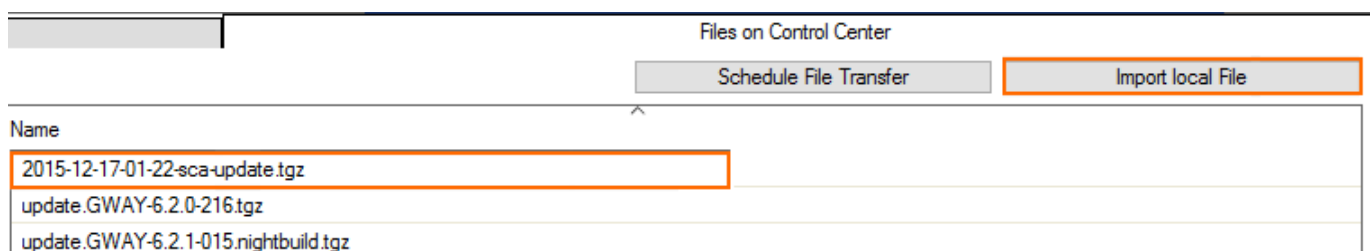
Step 2. Download the Update Package from the Download Portal

Download the update package from the Barracuda Download Portal:
<https://dlportal.barracudanetworks.com>.

Step 3. Import the Update Package into the Control Center

Import the update file 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 **Files on Control Center** tab.
4. Click **Import local File** and select the update package you downloaded in Step 1.



The file is copied to the Control Center and displayed in the **Files on Control Center** tab.

Step 4. Send the Update Package to the Systems

1. On the **Firmware Update** page, select the Secure Connectors you want to update.
2. In the **Files on Control Center** tab, select the update package.
3. Click **Create Update Task**. The **New Update Task** window opens.
4. (optional) Select the **Scheduling Mode**.

5. Click **OK**.


The update packages are now copied to the selected remote systems. Go to **CONTROL > Update Tasks** to monitor the progress.

Box	Cluster	Range ID	Σ	RPM	Info	Status	Time	Reason
4: Group 4								
SC1	S-SeriesCluster	3	➤	2016-01-26-15-39-sca-update.tgz	10.33.0.1	0: Pending Copy		T Waiting..

Step 5. Execute the Update Package

After the update package has been copied to the Secure Connector, trigger the update.

1. Go to **CONTROL > Update Tasks**.
2. In the Σ column, a green icon is displayed that verifies that the update package was sent successfully.
3. Right-click the selected Secure Connector and select **Perform Update**.

Box	Cluster	Range ID	Σ	RPM	Info	Status	Time	Reason
1: Group 1								
FSC1	S-SeriesCluster	3		2016-01-26-15-39-sc-update.t...	10.22.0.1	2: Completed Copy		T Waiting...

Refresh

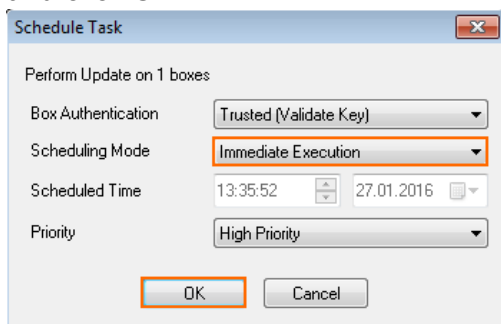
Perform Update

Delete Update

Arrange Icons By ▶

Tools ▶

4. In the **Schedule Task** window, select **Immediate Execution** from the **Scheduling Mode** list and click **OK**.



Wait for the update to finish.

Secure Connectors will reboot after the update has been applied.

Step 6. Migrate the SC Release Version

If you are updating to a new major version Secure Connector firmware, you must migrate the Secure Connector editor to the new version.

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > your range > your cluster > Cluster Settings**.
2. Right-click **Secure Connector Editor** and select **Lock**.
3. Right-click **Secure Connector Editor** and select **Migrate SC Release**.
4. Select the new **Release** version.
5. Click **OK**.
6. Click **Activate**.

Troubleshooting / Logs

To troubleshoot updates on the Secure Connector, you must enable **persistent logging** and review the **/var/phion/logs/installUpdate.log** file. Do not permanently enable persistent logging because it impacts the lifespan of the SD card.

Figures

1. import_update.png
2. create_update.png
3. Bild 009.png
4. FW_Update_01.png
5. FW_Update_02.png

© Barracuda Networks Inc., 2019 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.