

Secure Connector Firmware Updates

<https://campus.barracuda.com/doc/96026771/>

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. Firmware updates can be performed via Control Center and the web interface.

Perform a Firmware Update via the Control Center

Before You Begin

Verify the compatibility of the Secure Connector with the Control Center firmware. The Control Center firmware version must support 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](#).

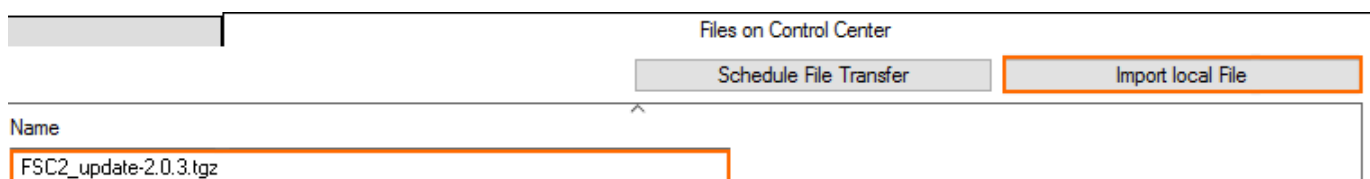
Step 1. Download the Update Package from the Download Portal

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

Step 2. 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.



Files on Control Center

Schedule File Transfer Import local File

Name

FSC2_update-2.0.3.tgz

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

Step 3. Send the Update Package to the Systems

1. On the **Firmware Update** page, select the Secure Connectors you want to update.
2. Right-click the selection and click **Select for Update**.

Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
Box	Version	Hotfixes	IP	Unit Description	Primary Server	Secondary Server	Last Status	File T
AAAA...	1.1		10.8.0.9				✓	
Conta...	1.1		10.8.0.8				✓	
Delet...	1.1		10.8.0.4				✓	
FSC1	FSC-2.0.3		10.8.0.3				✓ 24.10.2018 14:42:05	
NewB...	FSC-2.0.4		10.8.0.2				✓	
Single...	1.1		10.8.0.7				✓	
Templ...	1.1		10.8.0.5				✓	
UseT...	FSC-2.0.3		10.8.0.6				✓	
ccc	FSC-2.0.7		10.8.0.1				✓	
1/ [Regr...	7.2							
Clone...	FSC-2.0.6		10.15.0.7				✓	
Delet...	2.0		10.15.0.11				✓	
SCACR...			10.17.74.217		S1_Regression_1		✓ 04.06.2019 11:04:09	
SC1T...	1.1		10.15.0.4				✓	
SC1T...	FSC-1.1.5		10.15.0.3				✓	
SC2T...	FSC-2.0.5						✓	
SC2...	FSC-2.0.7						✓	

Selected Units for new Update Task

Box

Version

Hotf

Unit Description

Primary Server

Secondary Server

Last Status

Select for Update

Perform Update

Delete Update

Show Details

3. The Secure Connectors are now listed under **Selected Units for new Update Task**.

Selected Units for new Update Task					
Box	Version	Hotfixes	IP	Unit Description	Primary Server
 SC1Test	FSC-1.1.5		10.15.0.3		
 SC2TemplateTest	FSC-2.0.5		10.15.0.2		

4. In the **Files on Control Center** tab, select the update package.
5. Click **Schedule File Transfer**. The **New Update Task** window opens.
6. (optional) Select the **Scheduling Mode**.

New Update Task

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

Files

FSC2_update-2.0.3.tgz

Settings

Box Authentication: Trusted (Validate Key)

Scheduling Mode: Immediate Execution

Scheduled Time: Delayed Execution

Priority: High Priority

Boxes

Box	Cluster	Range
SC1Test	[Regr...	1
SC2Templat...	[Regr...	1

OK Cancel

7. Click **OK**.

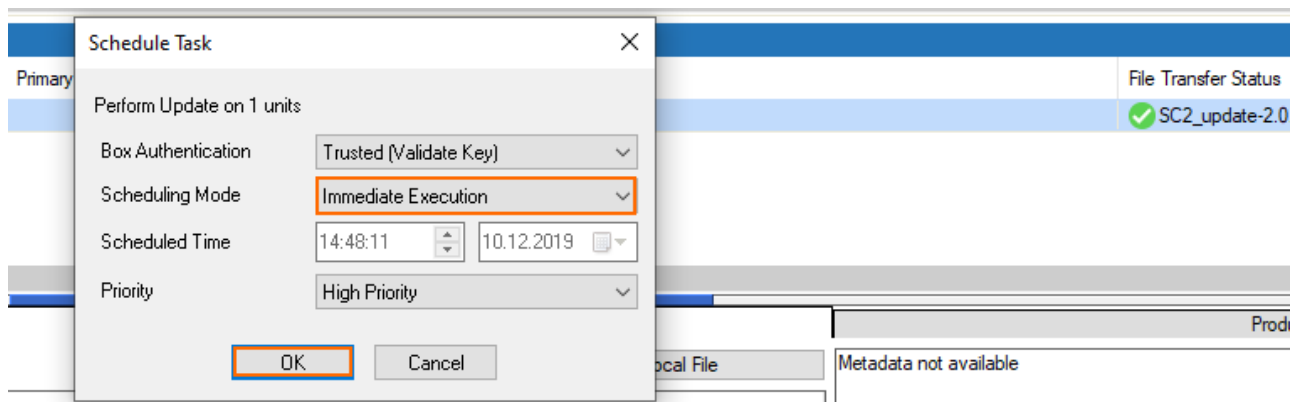
The update packages are now copied to the selected remote systems. The **File Transfer Status**

column shows the progress.

Step 4. Execute the Update Package

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

1. In the **Selected Units for new Update Task** column, a green icon is displayed that verifies that the update package was sent successfully.
2. Right-click the selected Secure Connector and select **Perform Update**.
3. In the **Schedule Task** window, select **Immediate Execution** from the **Scheduling Mode** list and click **OK**.



Wait for the update to finish.

The Secure Connectors will reboot after the update has been applied.

Step 5. 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.

Perform a Firmware Update via Web Interface

Before You Begin

Verify the compatibility of the Secure Connector with the Control Center firmware. The Control Center firmware version must support 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 1. Download the Update Package from the Download Portal

1. In your web browser, go to `https://<management IP address of your Secure Connector>`
2. Sign in using your Secure Connector **Username** and **Password**. The web interface opens showing the **Dashboard** tab.
3. Click **Retrieve Lock** in the upper-right corner of the **Dashboard** window.
4. In the **Firmware Update** section, click **Download Update**.

The update package is now downloaded as backup.conf file from the Barracuda Download Portal.

Step 2. Apply the Firmware Update

1. On the **Dashboard** page, click **Choose File** in the **Firmware Update** section.
2. Select the backup.conf file containing the firmware update
3. Click **Apply Backup**. The backup gets now installed.
4. Wait until this process has finished, then click **Release Lock** in the upper-right corner of the **Dashboard** window.

The update package has now been applied to your Secure Connector and gets recognized by the managing Control Center.

Figures

1. import_update.png
2. sc_select_for_update.png
3. sc_selected_for_update.png
4. sc_file_trans.png
5. sc_perform_update.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.