

How to Back Up and Restore Firewall, Secure Access Controller and Control Center Configurations

<https://campus.barracuda.com/doc/79463394/>

To back up and restore your system, you must create a Portable Archive (PAR) file. A Barracuda CloudGen Firewall running firmware 6.0.1 or higher can also create encrypted PCA files to store the system configuration.

File Type	PAR File	Comment	Restore Configuration via...
PAR	uncompressed, unencrypted archive file	This is the default option.	Barracuda Firewall Admin, /opt/phion/update/, USB stick when using Barracuda F-Series Install
PGZ	compressed, unencrypted archive file	Can only be created via Barracuda Firewall Admin.	Barracuda Firewall Admin, /opt/phion/update
PCA	encrypted archive file	CloudGen Firewall and Firewall Control Center version 6.0.1 or higher.	Barracuda Firewall Admin. If the password is set to the serial number of the appliance, you can also restore via /opt/phion/update/ or USB stick when using F-Series Install

Stand-Alone CloudGen Firewall and Stand-Alone Secure Access Controller

Create a PAR or PCA file to back up and restore the configuration of a stand-alone CloudGen Firewall or a stand-alone Secure Access Controller.

Back Up the CloudGen Firewall or Secure Access Controller

1. Go to **CONFIGURATION > Configuration Tree**.
2. Right-click **Box** and select **Create PAR file**. The **Save As** window opens.
3. Select the archive type:
 - **PAR File (*.par)** (default)
 - **Compressed PAR File (*.pgz)**
 - **Encrypted PAR File (*.pca)**
4. If you selected **Encrypted PAR file**, the **Password** window opens.
5. Click **Use Serial Number**, or enter the **Password** manually.

PCA archives with manual passwords cannot be used to reinstall your CloudGen Firewall or Control Center via F-Series Install or update the configuration via /opt/phion/update. Decrypt the archive manually for these operations. For more information, see [phionar and conftool](#).

Restore the CloudGen Firewall or Secure Access Controller

1. Go to **CONFIGURATION > Configuration Tree**.
2. Right-click **Box** and select **Restore from PAR file**. Select the required PAR / PGZ / PCA file.
3. If you are using a PCA file, enter the **Password** and click **OK**.
4. Click **Activate**.
5. Go to **CONTROL > Box**.
6. In the left navigation pane, expand **Operating System** and click **Firmware Restart**.
Click **Yes** to confirm that you want to restart the subsystem.
7. Expand **Network** and click **Activate new network configuration**.
8. Activate the new network configuration:
 - If you are continuing to use the same management IP address and management port, click **Failsafe**.
 - If the new network configuration uses a new management IP address, click **Activate Now**.
For information, see [How to Activate Network Changes](#).

PAR files can also be created from the CLI. For more information, see [How to Create PAR or PCA Files on the Command Line](#). If the PAR file should be used for the setup process, copy the PAR file to the USB flash drive that you will use for installation. You can only copy one PAR file on the USB flash drive. You must name the file as **box.par**.

Barracuda Firewall Control Center

Two PAR files are needed to back up your Firewall Control Center: the box layer box.par and the archive.par containing the Control Center configuration that includes all managed firewalls, the Secure Access Controller, and all Secure Connectors. You cannot restore a managed firewall from the archive.par directly.

If you are running a productive Control Center and a second Control Center for test purposes and both use the same configuration, you must change the Control Center ID on your test Control Center since the ID of each Control Center must always be unique. For more information, see [How to Generate a New Control Center ID](#)

Back Up the Control Center Box Layer

To back up the Firewall Control Center, you must create a PAR file for the box layer and the archive.par for the Control Center configuration.

1. Log into the box layer of the Control Center.

2. Go to **CONFIGURATION > Configuration Tree**.
3. Right-click **Box** and select **Create PAR file**. The **Save As** window opens.
4. Select the archive type:
 - **PAR File (*.par)** (default)
 - **Compressed PAR File (*.pgz)**
 - **Encrypted PAR File (*.pca)**
5. If you selected **Encrypted PAR file**, the **Password** window opens.
6. Click **Use Serial Number** or enter the **Password** manually.

The **box.par** file is saved to your local hard drive.

Back Up the Control Center Configuration

1. Log into the Control Center.
2. Go to **CONFIGURATION > Configuration Tree**.
3. Right-click the **Multi-Range** and select **Create PAR file**.
4. The **Save As** window opens.
5. Select the archive type:
 - **PAR File (*.par)** (default)
 - **Compressed PAR File (*.pgz)**
 - **Encrypted PAR File (*.pca)**
6. If you selected **Encrypted PAR file**, the **Password** window opens.
7. Click **Use Serial Number** or enter the **Password** manually.

The **archive.par** file is saved to your local hard drive.

Restore the Control Center Box Layer

To restore the Control Center:

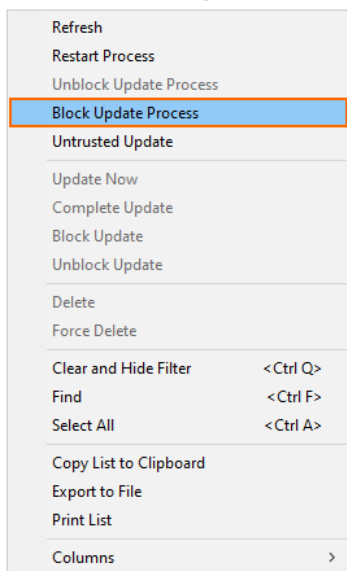
1. Log into the box layer of the Control Center.
2. Go to **CONFIGURATION > Configuration Tree**.
3. Right-click **Box** and select **Restore from PAR file**. Select the required PAR / PGZ / PCA file.
4. If you are using a PCA file encrypted with a manual password, enter the **Password** and click **OK**.
5. Click **Activate**.
6. Go to **CONTROL > Box**
7. In the left navigation menu, expand **Operating System** and click **Firmware Restart**.
Click **Yes** to confirm that you want to restart the subsystem.
8. Expand **Network** and click **Activate new network configuration**.
9. Select one of the following network configuration activation modes:
 - If you are continuing to use the same management IP address and management port, click **Failsafe**.
 - If the new management IP address and management port are different from the ones currently configured on the appliance, click **Activate now**.

For information, see [How to Activate Network Changes](#).

Restore the Control Center Configuration

In order to prevent the Control Center from accidentally sending configuration updates to the managed firewalls while restoring the PAR file, it is recommended to block the update process:

1. Log into the Control Center.
2. Go to **CONTROL > Configuration Updates**.
3. Right-click into the main display area of the window.
4. A list is displayed.
5. Select **Block Update Process** from the list.



It is now safe to restore the PAR file:

1. Go to the **CONFIGURATION > Configuration Tree** page. If you are prompted with warning messages, click **no**.
2. Right-click **Multi-Range** and select **Restore from PAR file**.
3. Select the required **archive.par** file.
4. (Optional) If the license has changed, you must also import the base license of the box layer on the Control Center. For more information, see [How to Manually Install the Licenses for the Control Center](#).

If you are restoring the configuration of a Control Center that has been reinstalled after a system crash, you must also restore the configurations of the appliances that it manages.

After restoring the PAR file, configuration updates must be unblocked:

1. Go to **CONTROL > Configuration Updates**.

2. Right-click into the main display area of the window.
3. A list is displayed.
4. Select **Unblock Update Process**.

Managed CloudGen Firewalls and Managed Secure Access Controller

To back up and restore the configuration of a CloudGen Firewall or Secure Access Controller that is managed by the Control Center, you must create a PAR file in the Control Center and then recover the managed firewall directly.

Back Up the Managed CloudGen Firewall or the Managed Secure Access Controller

1. Log into the Control Center.
2. Click the **CONFIGURATION** tab.
3. In the **Configuration Tree**, navigate to the range and cluster for the CloudGen Firewall or the Secure Access Controller.
4. Expand **Boxes**, right-click the CloudGen Firewall or the Secure Access Controller, and select **Create PAR file for box**.
5. Select the archive type:
 - **PAR File (*.par)** (default)
 - **Compressed PAR File (*.pgz)**
 - **Encrypted PAR File (*.pca)**
6. If you selected **Encrypted PAR file**, the **Password** window opens.
7. If you selected **Encrypted PAR file**, click **Use Serial Number** or enter the **Password** manually.
8. Save the PAR file to your local hard drive.

Restore the Managed CloudGen Firewall or the Managed Secure Access Controller

1. Log into the CloudGen Firewall or the Secure Access Controller.
2. Go to the **CONFIGURATION > Configuration Tree** page.
3. Right-click **Box** and select **Restore from PAR file**. Select the PAR or PCA file you previously created for this firewall in the Control Center.
4. If you are using a PCA file encrypted with a manual password, enter the **Password** and click **OK**.
5. Click **OK** to confirm the Emergency Override warning message.
6. Click **Activate**.
7. Go to the **CONTROL > Box** page.
8. In the left navigation pane, expand **Operating System** and click **Firmware Restart**. Click **Yes** to confirm that you want to restart the subsystem.
9. Expand **Network** and click **Activate new network configuration**.
10. Select one of the following network configuration activation modes:
 - If you are continuing to use the same management IP address and management port, click **Failsafe**.

- If the new management IP address and management port are different from the ones currently configured on the appliance, click **Activate now**.
For information, see [How to Activate Network Changes](#).

Further Information

- [How to Back Up and Restore CC Archive PAR Files on the Command Line](#)
- [How to Create PAR or PCA Files on the Command Line](#)

Figures

1. block_update_process.png

© Barracuda Networks Inc., 2021 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.