Automated Critical Updates

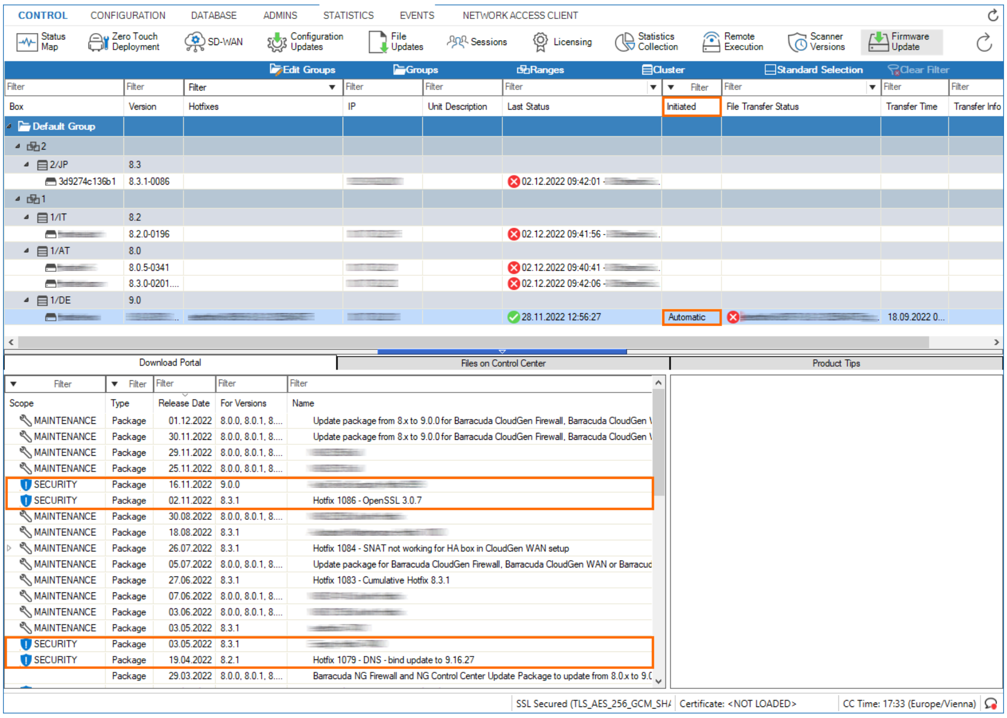
https://campus.barracuda.com/doc/98214584/

Automated Critical Updates is a new feature that allows you to configure scheduled security updates. It is activated by default on firmware 9.0.0. The feature runs on Control Centers and both managed and stand-alone firewalls. Running the feature on the box level of a Control Center is the same as running the feature on a stand-alone firewall.

When Barracuda Networks provides a security update, the related file becomes available on the Barracuda Download Portal. The Automated Critical Updates feature automates the manual steps for selecting these files to maximize security and for downloading them to the Control Center or a stand-alone firewall based on the configured time frames for the installation.

The window for firmware updates also displays the availability and the status of automated critical updates in two views at **CONTROL > Firmware Updates**:

1. Top view – The upper half of the view shows the status of the security updates in the column **Initiated** by the entry **Automatic**.
2. Lower-left view – The lower-left view contains one or more entries that contain the label **SECURITY** in the column **SCOPE**.



Box	Version	Hotfixes	IP	Unit Description	Last Status	Initiated	File Transfer Status	Transfer Time	Transfer Info
Default Group									
2									
2/JP	8.3								
3d9274c136b1	8.3.1-0086		[redacted]		☒ 02.12.2022 09:42:01 - [redacted]				
1									
1/IT	8.2								
[redacted]	8.2.0-0196		[redacted]		☒ 02.12.2022 09:41:56 - [redacted]				
1/AT	8.0								
[redacted]	8.0.5-0341		[redacted]		☒ 02.12.2022 09:40:41 - [redacted]				
[redacted]	8.3.0-0201....		[redacted]		☒ 02.12.2022 09:42:06 - [redacted]				
1/DE	9.0								
[redacted]	[redacted]	[redacted]	[redacted]		✓ 28.11.2022 12:56:27	Automatic	☒ [redacted]	18.09.2022 0...	

Scope	Type	Release Date	For Versions	Name
MAINTENANCE	Package	01.12.2022	8.0.0, 8.0.1, 8....	Update package from 8.x to 9.0.0 for Barracuda CloudGen Firewall, Barracuda CloudGen \
MAINTENANCE	Package	30.11.2022	8.0.0, 8.0.1, 8....	Update package from 8.x to 9.0.0 for Barracuda CloudGen Firewall, Barracuda CloudGen \
MAINTENANCE	Package	29.11.2022	8.0.0, 8.0.1, 8....	[redacted]
MAINTENANCE	Package	25.11.2022	8.0.0, 8.0.1, 8....	[redacted]
SECURITY	Package	16.11.2022	9.0.0	[redacted]
SECURITY	Package	02.11.2022	8.3.1	Hotfix 1086 - OpenSSL 3.0.7
MAINTENANCE	Package	30.08.2022	8.0.0, 8.0.1, 8....	[redacted]
MAINTENANCE	Package	18.08.2022	8.3.1	[redacted]
MAINTENANCE	Package	26.07.2022	8.3.1	Hotfix 1084 - SNAT not working for HA box in CloudGen WAN setup
MAINTENANCE	Package	05.07.2022	8.0.0, 8.0.1, 8....	Update package for Barracuda CloudGen Firewall, Barracuda CloudGen WAN or Barracuc
MAINTENANCE	Package	27.06.2022	8.3.1	Hotfix 1083 - Cumulative Hotfix 8.3.1
MAINTENANCE	Package	07.06.2022	8.0.0, 8.0.1, 8....	[redacted]
MAINTENANCE	Package	03.06.2022	8.0.0, 8.0.1, 8....	[redacted]
MAINTENANCE	Package	03.05.2022	8.3.1	[redacted]
SECURITY	Package	03.05.2022	8.3.1	[redacted]
SECURITY	Package	19.04.2022	8.2.1	Hotfix 1079 - DNS - bind update to 9.16.27
	Package	29.03.2022	8.0.0, 8.0.1, 8....	Barracuda NG Firewall and NG Control Center Update Package to update from 8.0.x to 9.(

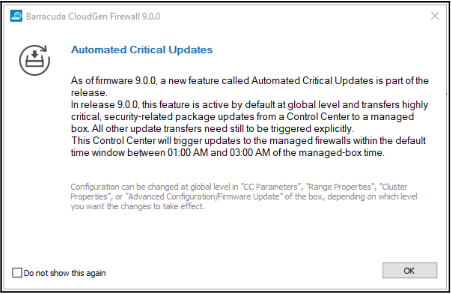
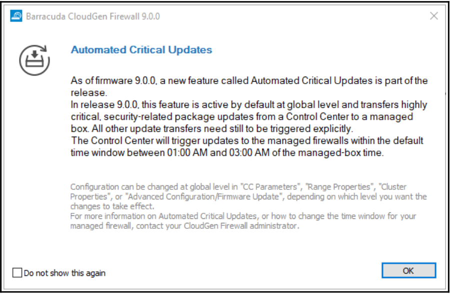
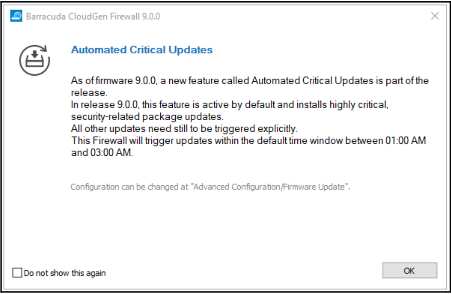
SSL Secured (TLS_AES_256_GCM_SH/ Certificate: <NOT LOADED> CC Time: 17:33 (Europe/Vienna)

You can still inspect the status and stop updates in the Schedule view.

Notification of Activated Feature upon Login

Because automated critical updates are activated by default on firmware 9.0.0, you will see a notification window upon your first login informing you that the feature is already running and where to configure the feature depending on the type of your appliance. The timeframe in which automated critical updates take place is preset from 1:00 AM to 3:00 AM. You can deactivate this dialog notification window by selecting the check box in the lower-left corner.

Note the different announcements in the dialog window that refer to the related configuration node on each of these three different instances:

Notification on a Control Center	Notification on a Managed Firewall	Notification on a Standalone Firewall / CC Box Level
 Barracuda CloudGen Firewall 9.0.0 Automated Critical Updates As of firmware 9.0.0, a new feature called Automated Critical Updates is part of the release. In release 9.0.0, this feature is active by default at global level and transfers highly critical, security-related package updates from a Control Center to a managed box. All other update transfers need still to be triggered explicitly. This Control Center will trigger updates to the managed firewalls within the default time window between 01:00 AM and 03:00 AM of the managed-box time. Configuration can be changed at global level in "CC Parameters", "Range Properties", "Cluster Properties", or "Advanced Configuration/Firmware Update" of the box, depending on which level you want the changes to take effect. ☐ Do not show this again OK	 Barracuda CloudGen Firewall 9.0.0 Automated Critical Updates As of firmware 9.0.0, a new feature called Automated Critical Updates is part of the release. In release 9.0.0, this feature is active by default at global level and transfers highly critical, security-related package updates from a Control Center to a managed box. All other update transfers need still to be triggered explicitly. The Control Center will trigger updates to the managed firewalls within the default time window between 01:00 AM and 03:00 AM of the managed-box time. Configuration can be changed at global level in "CC Parameters", "Range Properties", "Cluster Properties", or "Advanced Configuration/Firmware Update", depending on which level you want the changes to take effect. For more information on Automated Critical Updates, or how to change the time window for your managed firewall, contact your CloudGen Firewall administrator. ☐ Do not show this again OK	 Barracuda CloudGen Firewall 9.0.0 Automated Critical Updates As of firmware 9.0.0, a new feature called Automated Critical Updates is part of the release. In release 9.0.0, this feature is active by default and installs highly critical, security-related package updates. All other updates need still to be triggered explicitly. This Firewall will trigger updates within the default time window between 01:00 AM and 03:00 AM. Configuration can be changed at "Advanced Configuration/Firmware Update". ☐ Do not show this again OK

For security reasons, Barracuda Networks recommends keeping the feature activated. However, if you do not want to use it, you can deactivate it at the corresponding node in the configuration tree.

Configuration of Automated Critical Updates

The configuration of automated critical updates is preset for all relevant parameters in the configuration window. However, the node for this configuration window varies depending on what appliance the configuration has to be made on.

Configuration Node on a Control Center	Configuration Node on a Managed Firewall	Configuration Node on a Stand-alone Firewall / CC Box Level

• **Global Level** ◦ **CONFIGURATION > Configuration Tree > Global Settings > CC Parameters** • **Range Level** ◦ **CONFIGURATION > Configuration Tree > Global Settings > *your Range* > Range Properties** • **Cluster Level** ◦ **CONFIGURATION > Configuration Tree > Global Settings > *your Range* > *your Cluster* > Cluster Properties**	**CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Firmware Update** Note: the settings at this node are managed on the corresponding node in the managing Control Center.	**CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Firmware Update**

Apart from Control Center-specific services, a Control Center is basically a stand-alone firewall at the box level and therefore has the same configuration nodes in the configuration tree as a stand-alone firewall. For this reason, the configuration node **Firmware Update** is the same for each of them. On managed firewalls, however, you will see a warning dialog window informing you that the configuration is managed by a related Control Center if you make an attempt to lock the node for modification.

Also, because a managed firewall is subordinated to its related Control Center, its settings for firmware updates depend on whether the configuration is related to a specific cluster or range. The managed firewall will therefore receive the configuration that contains the schedule for updates from the settings configured either at the global, range, or cluster level. In addition, these settings can also be overridden as described below.

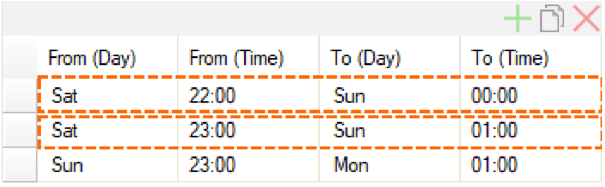
Time Frames and Schedule

Time frames are essential for performing automated critical updates on any firewall / Control Center. Because the beginning of a time frame indicates when exactly the Control Center must check the availability of new security updates, the effective update time can be delayed.

A time frame is defined by the beginning and end time, and can be configured individually. For the purpose of automated critical updates, the following parameters must be configured:

- **From (Day)** – The day of the week (Mon, Tue, ...)
- **From (Time)** – Time stamp in 24h format
- **To (Day)** – The day of the week (Mon, Tue, ...)
- **To (Time)** – Time stamp in 24h format

You can enter multiple time frames. A time frame may exceed a single day. If time frames overlap, they are regarded as single, connected time frame. The following image shows two time frames that overlap. The effective time frame therefore begins on Saturday at 22:00, and ends on Sunday at 01:00. All three time frames together build a schedule.

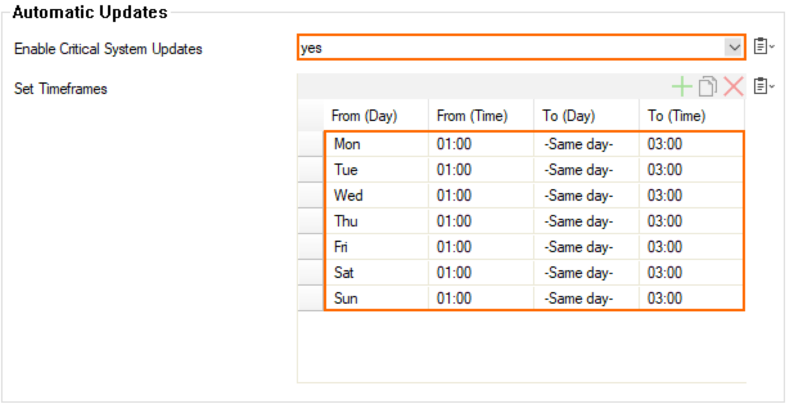


From (Day)	From (Time)	To (Day)	To (Time)
Sat	22:00	Sun	00:00
Sat	23:00	Sun	01:00
Sun	23:00	Mon	01:00

A schedule for automated critical updates may be configured both on stand-alone firewalls and on the box level of Control Centers, and on the CC levels of **Global**, **Range**, and **Cluster**.

Automated Security Update Schedules on a Stand-alone Firewall and on Box Level of a Control Center

On a stand-alone firewall or on the box level of a Control Center, you can configure a schedule for automated critical updates at **CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Firmware Update**. The schedule in the following image also shows the standard preset configuration.



Automatic Updates

Enable Critical System Updates: yes

Set Timeframes

From (Day)	From (Time)	To (Day)	To (Time)
Mon	01:00	-Same day-	03:00
Tue	01:00	-Same day-	03:00
Wed	01:00	-Same day-	03:00
Thu	01:00	-Same day-	03:00
Fri	01:00	-Same day-	03:00
Sat	01:00	-Same day-	03:00
Sun	01:00	-Same day-	03:00

To use the feature, select **yes** for **Enable Critical System Updates**. The firewall will then contact the update server and download the security updates if there are any present.

Inherited, Push, or Pull – How the Control Center Uses Metadata to Control Automated Critical Updates for Managed Firewalls

Metadata is data that provides basic information about certain content without any content details.

For automated critical updates, this means that metadata contains information about the availability of certain update files and where they can be found but not the update file itself.

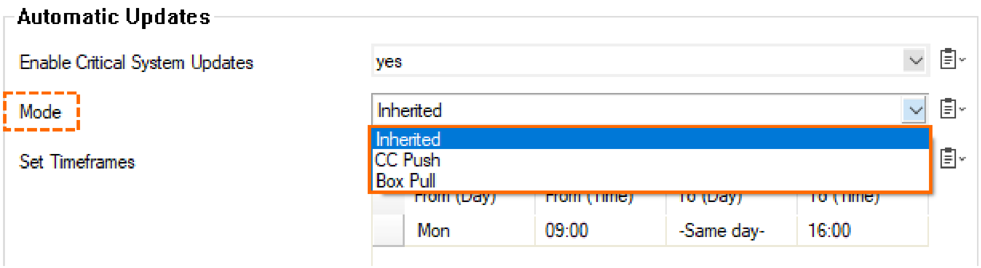
Because the Control Center handles settings on the global, range, and cluster levels, the settings for automated critical updates are present on all three configuration levels at the nodes, as listed in the table above. In order to configure the feature with maximum flexibility for all managed firewalls, you have the option of inheriting the settings from the global level to the range level and from the range level to the cluster level. To do so, select the third option from the menu list for the mode: **Inherited**.

As a consequence, the Control Center handles automated critical updates in three different ways. These three **Mode** options are named in the user interface as shown in the table below. You can decide which mode best matches your requirements:

Mode	Meaning	Note
Inherited	Ignore the following two options and apply the configuration settings of the parent configuration level.	This option does not apply to the global level in the configuration tree and is only available on the range and cluster levels.
CC Push (default preset)	The Control Center downloads all available security update files from the download portal locally and sends them to the managed firewall according to the schedule of its own configuration level.	The Control Center must be permanently available for the managed appliances. If the connection gets interrupted, the managed appliances cannot be updated. **Pros:** • The Control Center downloads and manages the updated files and manages the complete update process for all managed appliances. • As long as the connection does not break, the Control Center will always display the current update status of the managed appliances. **Cons:** • The managed firewalls are fully dependent on the settings configured and maintained centrally on the Control Center. • If the connection to the Control Center gets interrupted, the managed firewalls will not be updated.

Box Pull	The managed firewall receives the metadata from the managing Control Center and downloads the security update files from the download portal according to the locally configured schedule. This mode overrides any preset that is propagated from a higher configuration level in the configuration tree of the Control Center and takes the schedule from its own configuration level. Schedules from the range or cluster level are ignored.	Temporary disconnections of the managed firewalls from the Control Center will not prevent the firewalls from downloading updates provided that the firewalls do not lose their connection to the update servers. **Pros:** • The managed boxes receive metadata from the Control Center, and the managed appliances will download the update files themselves, even if the connection to the Control Center gets interrupted. The update status is reported back to the Control Center when the connection is available. **Cons:** • If the connection of a managed appliance to the Control Center is interrupted, the managed appliances will not be able to receive information for their updates. Also, the managed appliances will not be able to report their current update status to the related Control Center.

From the list, select the **Mode** that best fits your requirements.



Automatic Updates

Enable Critical System Updates: yes

Mode: Inherited

Set Timeframes

From (Day)	From (Time)	To (Day)	To (Time)
Mon	09:00	-Same day-	16:00

Note that the modes **CC Push** and **Box Pull** both relate to the Control Center so that it can receive feedback from the managed appliances about the status of the updating process.

The following table shows which configured values will be relevant for managed boxes depending on the **Mode** option at each corresponding level in the configuration tree:

Config Level	**Update Node**	**Mode**	**Preset**	**Meaning**
Global	CC Parameters	-		-
		CC Push	*	Control Center sends security updates to the managed box.
		Box Pull		Managed firewall receives metadata from the CC and downloads the security update itself according to the local schedule.

Range	Range Properties	Inherited	*	Both CC Push settings and Box Pull settings are taken from the global settings.
		CC Push		Control Center sends security updates to the managed box.
		Box Pull		Managed firewall receives metadata from the CC and downloads the security update itself according to the local schedule.
Cluster	Cluster Properties	Inherited	*	Both CC Push settings and Box Pull settings are taken from the range settings.
		CC Push		Control Center sends security updates to the managed box.
		Box Pull		Managed firewall receives metadata from the CC and downloads the security update itself according to the local schedule.
Box	Firmware Update	Inherited	*	Both CC Push settings and Box Pull settings are taken from the cluster settings.
		CC Push		Control Center sends security updates to the managed box.
		Box Pull		Managed firewall receives metadata from the CC and downloads the security update itself according to the local schedule.

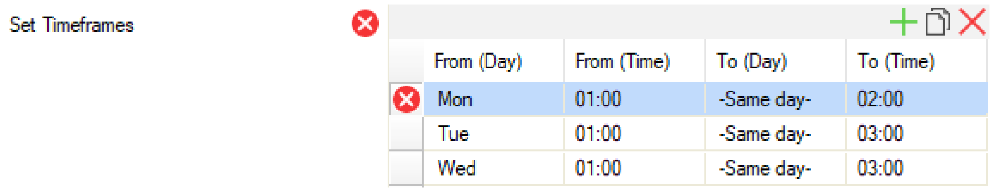
Preset Configuration Values

The preset values for Automated Critical Updates apply only to managed firewalls and not to stand-alone firewalls:

- **Enable Critical System Updates** – **yes**.
- **Mode**
  - **On global CC Level – CC Push.**
  - **On Range, Cluster, and Box level** – **Inherited**.
- **Set Time frames** – **Mon - Sun, 01:00 - 03:00**.

Note that the preset value of 01:00 - 03:00 has a duration of 2 hours, which is the minimum time required for performing security updates.

If you enter a time frame of less than 2 hours, a small red warning sign will appear.



Set Timeframes

From (Day)	From (Time)	To (Day)	To (Time)
Mon	01:00	-Same day-	02:00
Tue	01:00	-Same day-	03:00
Wed	01:00	-Same day-	03:00

CC-Managed HA Pairs

In order to not compromise the concept of HA, scheduling automated updates does consider that an HA pair will always be available. To do so, the Control Center first updates the secondary firewall and checks if the update was successful. If so, the primary firewall is then updated. If the secondary firewall encounters problems after an update, the primary firewall will not be updated in order to ensure further availability.

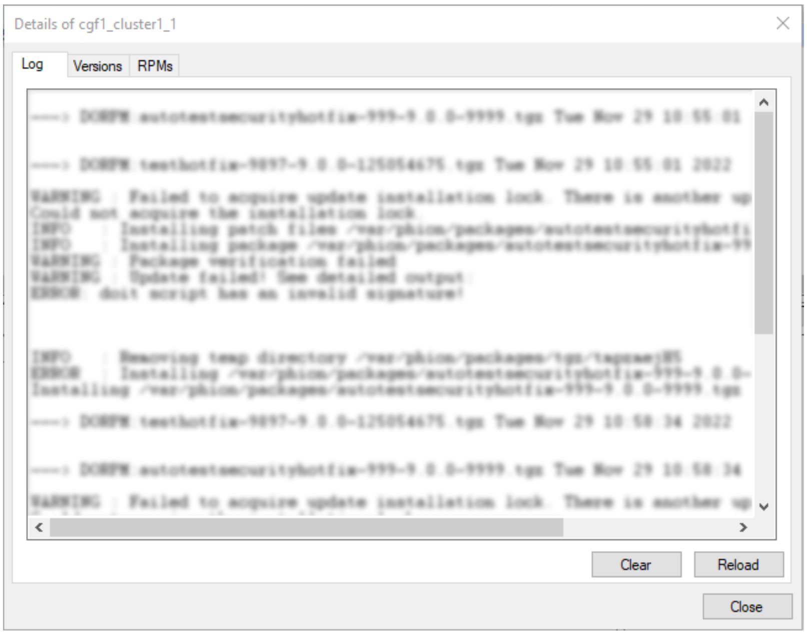
Note that if a reboot is required after a security update, no explicit notification will be sent. Details for a required reboot can be inspected in the maintenance window.

For more information on HA, see High Availability.

Logging, Status about Updates

The Automated Critical Updates feature sends messages to the log. These messages can be identified by the prefix `auto_firmware_update` and can be checked at **CONFIGURATION > LOGS > Box > Release > update**.

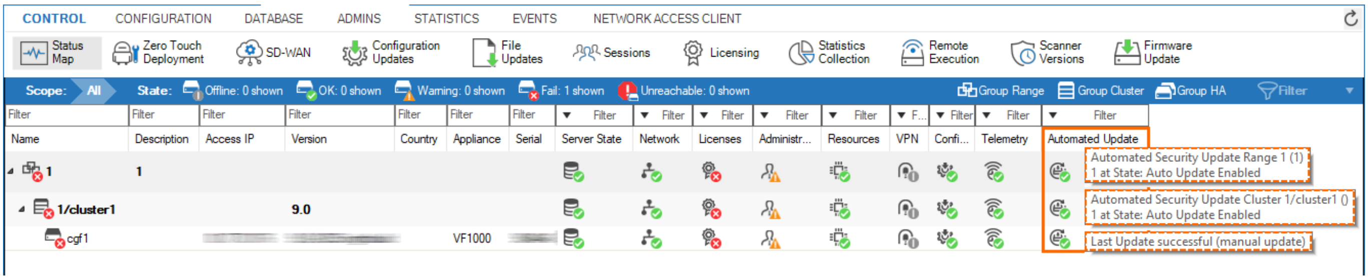
You can also get information about the status of the update log at **CONTROL > Firmware Updates**. Right-click your mouse on an entry of an automated update to display a list that contains the entry **Show Details**. Click this entry, and a window will open that shows details about the log, the versions, and the packages.



```
---> DORPM autotestsecurityhotfix-999-9.0.0-9999.tgz Tue Nov 29 10:55:01

---> DORPM testhotfix-9897-9.0.0-125054675.tgz Tue Nov 29 10:55:01 2022

WARNING : Failed to acquire update installation lock. There is another up
Could not acquire the installation lock.
INFO    : Installing patch files /var/phion/packages/autotestsecurityhotfi
INFO    : Installing package /var/phion/packages/autotestsecurityhotfix-99
WARNING : Package verification failed
WARNING : Update failed! See detailed output:
ERROR: doit script has an invalid signature!



INFO    : Removing temp directory /var/phion/packages/tgz/tagzaej85
ERROR   : Installing /var/phion/packages/autotestsecurityhotfix-999-9.0.0-
Installing /var/phion/packages/autotestsecurityhotfix-999-9.0.0-9999.tgz

---> DORPM testhotfix-9897-9.0.0-125054675.tgz Tue Nov 29 10:58:34 2022

---> DORPM autotestsecurityhotfix-999-9.0.0-9999.tgz Tue Nov 29 10:58:34

WARNING : Failed to acquire update installation lock. There is another up
```

Status View for Automated Updates

You can check the state of the Automated Critical Updates feature in the **Status Map** on the Control Center. The column **Automated Update** in the following screenshot shows the status for the range level, the cluster level, and the firewall subordinated to the cluster.



Name	Description	Access IP	Version	Country	Appliance	Serial	Server State	Network	Licenses	Administr...	Resources	VPN	Confi...	Telemetry	Automated Update
1	1						✓	✓	✗	⚠	✓	●	✓	✓	✓ Automated Security Update Range 1 (1) 1 at State: Auto Update Enabled
1/cluster1			9.0				✓	✓	✗	⚠	✓	●	✓	✓	✓ Automated Security Update Cluster 1/cluster1 () 1 at State: Auto Update Enabled
cgf1		[redacted]	[redacted]		VF1000	[redacted]	✓	✓	✗	⚠	✓	●	✓	✓	✓ Last Update successful (manual update)

Figures