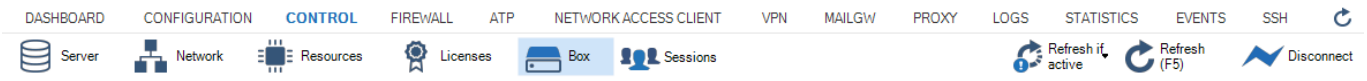
Box Page

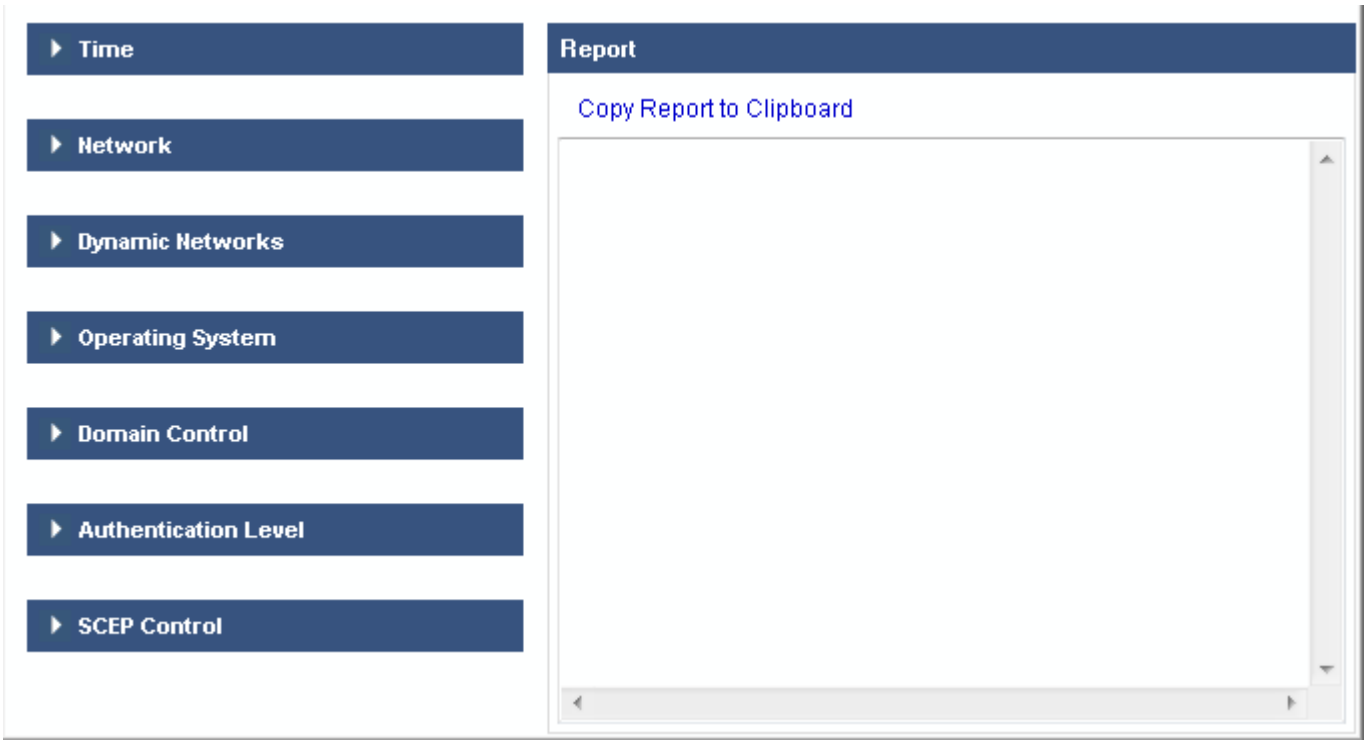
https://campus.barracuda.com/doc/73719524/

The **Box** page lets you configure and control key aspects of the CloudGen Firewall box operation. To access the **Box** page, open the **CONTROL** tab and click the **Box** icon in the ribbon bar.



The **Box** page consists of two sections:

- Configuration section
- Report section



Configuration Section

The **Configuration** section displays the following menus:

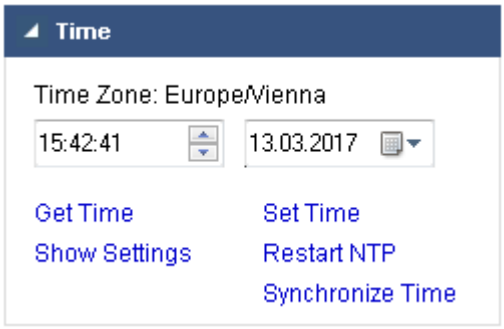
- **Time**
- **Network**
- **Dynamic Networks**
- **Operating System**

- **Domain Control**
- **Authentication Level**
- **SCEP Control**

To expand a menu, click on the triangle to the left.

Time

Expand the **Time** menu to display or change time settings.



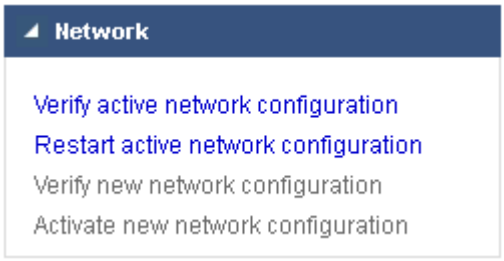
The menu offers the following options:

- **Get Time** – The current time and date on the firewall.
- **Show Settings** – The current NTP settings in the **Report** section.
- **Set Time** – Changes the current time and date to the values selected from the time and date fields. If your firewall is synchronized with an external time server, this manual change is overwritten by the succeeding time synchronization.
- **Restart NTP** – Restarts all NTP services.
- **Synchronize Time** – Offers an option dialog to synchronize the time settings with an NTP server.

If the **Using Time Server** and **Own IP** settings are unspecified, the synchronization process binds to the firewall's primary management IP address. This method works well with a time server that is placed in the same network as the primary management IP address. For time synchronization with a public time server, enter the external IP address of the firewall into the **Own IP** field so that the time server's response is not blocked by the firewall.

Network

Expand the **Network** menu to display or change network settings.



The menu offers the following options:

- Verify active network configuration
- Restart active network configuration
- Verify new network configuration
- Activate new network configuration

Verify Active Network Configuration

Click **Verify active network configuration** to see whether errors have been sent after successfully sending network configurations. Results appear in the **Report** section.

Restart Active Network Configuration

This option shuts down and then restarts the currently active network configuration.

The server subsystem is unaffected by this procedure, but the server and services will be unavailable for a short time while the network shuts down and restarts.

Verify New Network Configuration

Click **Verify new network configuration** to see whether errors have occurred after they have been successfully sent. Results appear in the **Report** section.

Changing the network configuration of a remotely controlled firewall is a critical operation. New network configurations are not automatically activated until after they have been verified. If the validation fails, correct the errors and verify the configuration again. The newly received network configuration is stored in `/opt/phion/preserve/boxnet.conf`.

Activate New Network Configuration

This option activates new network configurations after they have been successfully verified. You can activate the new network configuration in the following modes:

- **Activate now** – This option is offered when a management IP address has been changed. With this mode, the firewall activates the network change and reconnects to the new IP address.
- **Failsafe** – Failsafe network activation is the safest way to activate configuration changes. Always use this activation method on production firewalls

In Failsafe mode, the firewall creates a backup file of the active network configuration. It then temporarily activates the configuration changes and verifies that the firewall can still be contacted via Firewall Admin. If this verification is successful, the network is restarted so that the changes are activated permanently. If verification fails within the timeout defined in the **Set Timeout** field, the original network configuration is restored.

You might lose connection to the firewall, especially when activating network configuration changes via a VPN connection. This causes a connection verification failure between the firewall and Firewall Admin. As a result, the original configuration is then restored. If you experience this issue, try using **Force** network activation.

- **Force** – Forced network activation immediately activates the new network configuration with a logical consistency check, but without creating a backup file of the active network configuration.
- **Soft** – Soft network activation can be used only for IPv6 routes. For all other network changes a reboot of the firewall if required to complete the network activation after a soft activation.

For more information, see How to Activate Network Changes.

Dynamic Networks

If dynamic network connections have been configured, you can control them with options (off, on, start, stop, restart, reset) from the **Dynamic Networks** menu.

You can control the following types of network connections:

- xDSL
- ISDN
- DHCP (cable)-connections

- Wireless WAN (WWAN)
- MGMT (box management)
- Tunnel connections

Operating System

Expand **Operating System** to control the operating system.

The menu offers the following options:

- **Reboot Box** – Reboot the firewall.
- **Firmware Restart** – Shut down and restart all virtual servers and services belonging to the firewall subsystem, including the firewall engine.

All connections will be lost, including non-Barracuda proprietary services such as Secure Shell (SSHd) and Network Time Protocol (NTPd).

Using this option is similar to running the `/opt/phion/bin/phionctrl shutdown` and `/opt/phion/bin/phionctrl startup` commands, except the control daemon itself is not stopped and started.

- **Shutdown Box** – Turns off the firewall.
- **Save current Config for ART** – Saves the current configuration of the firewall to the ART crash recovery OS. If the firewall must be reinstalled remotely, it uses the current system configuration for the recovery process.
- **Install Update** – Installs the selected firmware updates, hotfixes, or patches. The update process can be triggered after the package is successfully uploaded to the unit.
- **Generate System Report** – Creates a system report.
- **Reset SMS Counter** – Resets the counter for the number of successive SMS commands that have been accepted by the interface.

Domain Control

From the **Domain Control** menu, you can register the firewall as a Windows domain member or view its domain registration status.

The menu provides offers following options:

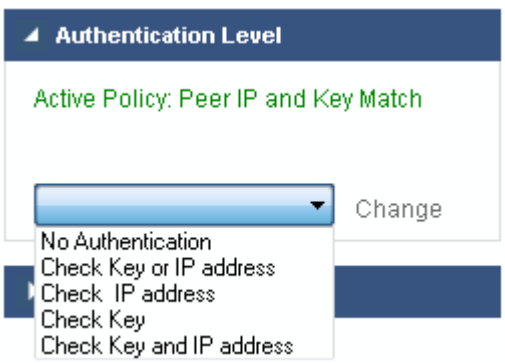
- **Show Registration Status** – Displays the registration status of the firewall at a Windows domain.
- **Register at Domain** – Registers the firewall as a Windows domain member at a domain controller. In the **User Authentication** window, enter the username and password for the user with the appropriate administrative rights to add the firewall to the domain. Before you can use this option, configure an Authentication service.
- **Register Proxy at Domain** – Registers the HTTP Proxy at the Windows domain.

Authentication Level

You can specify the level of authentication required for non-interactive Control Center logins and HA synchronization.

Authentication level changes take effect immediately.

Expand the **Authentication Level** menu to make changes to authentication.



The menu offers the following options:

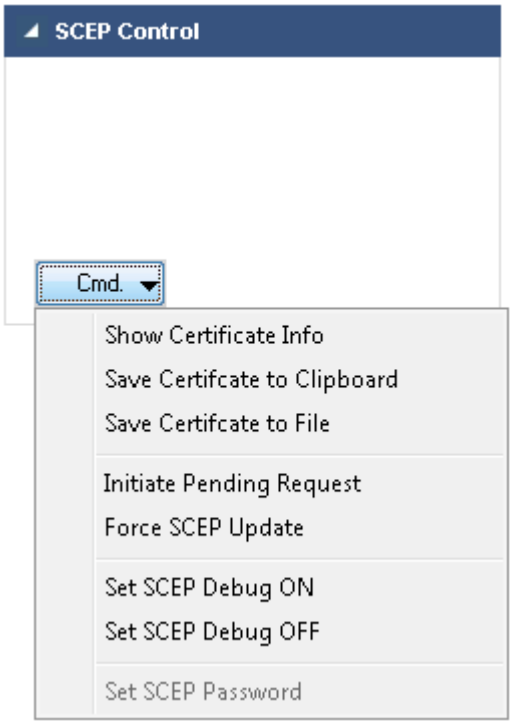
- **No Authentication** – Level -1. No authentication is required to send or retrieve configuration data.

Use this option only when necessary, and revoke it as soon as possible.

- **Check Key or IP address** – Level 0. An IP address or key challenge is required. This option is not considered to be secure.
- **Check IP address** – Level 1. This option is not considered to be secure.
- **Check Key** – Level 2. This option is not considered to be secure.
- **Check Key and IP address** – Level 3, the default setting. Do not change it unless you must temporarily lower the security level. A change might be required when either the IP addresses of the Control Center or HA partner change, or the key of the Control Center changes.

SCEP Control (Simple Certificate Enrollment Protocol)

You can view and configure SCEP settings.



Expand the **SCEP Control** menu to select the following options from the **Cmd** list:

- **Show Certificate Info** – Displays information about the certificate retrieved by SCEP.

- **Save Certificate to Clipboard** – Exports the certificate to the clipboard (PEM).
- **Save Certificate to File** – Exports the certificate to a file (PEM).
- **Initiate Pending Request** – Starts the enrollment process immediately.
- **Force SCEP Update** – Starts an SCEP update.
- **Set SCEP Debug ON** – Turns SCEP debugging on. Additional debugging information is included in the SCEP log (**Box > Control > SCEP**).
- **Set SCEP Debug OFF** – Turns SCEP debugging off.
- **Set SCEP Password** – Prompts for the SCEP password. This option is available only if the SCEP password policy is set to *Enter-Password-At-Box*.

Report Section

The **Report** section displays reporting information that has been queried in the Configuration section.

Figures

1. box_page_00.png
2. box_window_00.png
3. time_collapsed_00.png
4. network_collapsed_00.png
5. dynamic_networks_collapsed_00.png
6. operating_system_collapsed_00.png
7. domain_control_collapsed_00.png
8. authentication_level_collapsed_00.png
9. scep_collapsed_00.png