

Barracuda CloudGen Remote

<https://campus.barracuda.com/doc/73719580/>

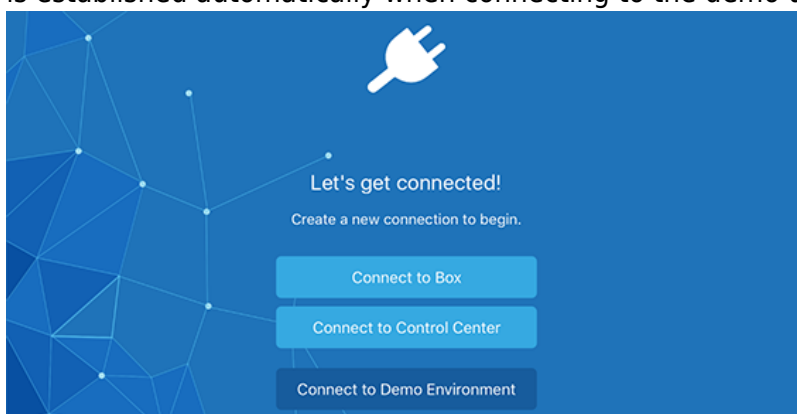
Barracuda Firewall Remote Control for Apple iOS provides system administrators easy remote access to their CloudGen Firewalls and Control Centers through their iOS device. Firewall Remote Control provides general information on the unit's status and allows system administrators to reboot the unit, restart all its services, reconnect the network, and rebuild management tunnels. The Dynamic Firewall Rules interface displays all configured dynamic firewall rules with options to enable/disable or temporarily enable those rules. Firewall Remote Control for Apple iOS lets you create a connection to one or more CloudGen Firewalls via a Firewall Control Center. Firewall Remote Control provides full terminal access via SSH.

Requirements

- Access to the management IP addresses, either directly or via client-to-site VPN.
- Firmware 6.0.1 or higher.

Adding a CloudGen Firewall or Control Center

1. Tap **New Connection** in the upper-left corner.
 1. Tap **Connect to Box** to add a CloudGen Firewall.
 2. Tap **Connect to Control Center** to add a Firewall Control Center.
 3. Tap **Add Demo via VPN** to add the Barracuda Networks demo units. This will also automatically install and configure a VPN connection profile to Barracuda Networks, which is established automatically when connecting to the demo units.



2. Enter a descriptive **Name** for the unit.
3. In the **Host** field, enter the Management IP address of your firewall or Control Center.
4. In the **Log In** and **Password** fields, enter the user credentials of the respective unit.
5. To add this unit to the list of favorites, store the password for fast connection or add to a specific group, and enable the respective parameters in the **Settings** and **Groups** section.

6. Tap **Save** in the upper-right corner to store this connection on your mobile device.

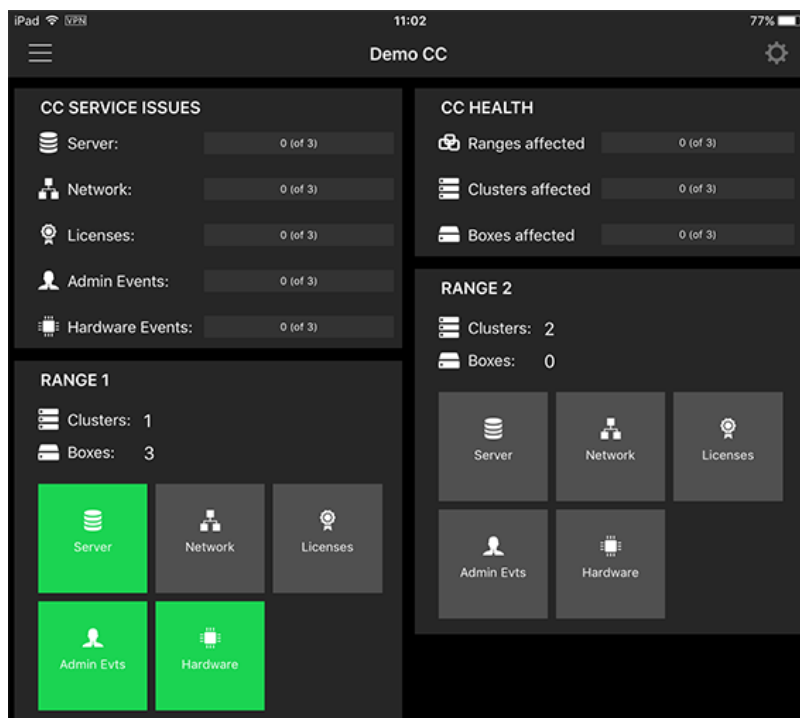
Connecting to your Firewall or Control Center

To connect to a unit via Firewall Remote Control , tap the entry in the left menu.

The Firewall Remote Control Status Page

Firewall Remote Control shows the status of the CloudGen Firewall or Control Center, including server/service control, CPU load, system, network control, events, and licenses.

The status page of the Control Center shows the range and cluster architecture and provides general information on the server and health status of the managed firewalls.

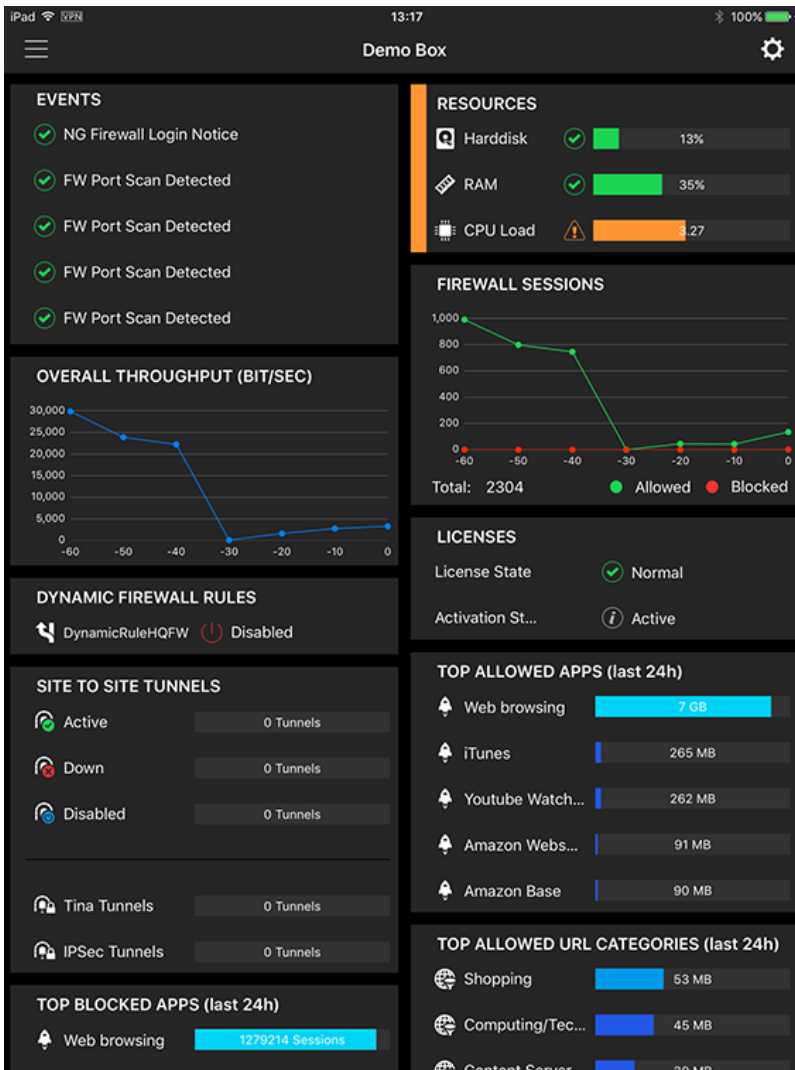


The status page offers the following features:

- **CC Service Issues** – This section provides general information on the unit's server and service status, CPU and system status, event status, license status, as well as kernel, link, and architecture.
- **CC Health** – This section displays the health status of the managed firewall units per range and cluster.

- **Range 1,2,3...** – Displays all ranges configured on the Control Center and shows the clusters and managed firewalls. Each range provides subsections, allowing access to all managed firewalls.

The status page of the firewall provides general information on the unit, such as name, current license and activation state, installed firmware version, appliance model, and serial number.



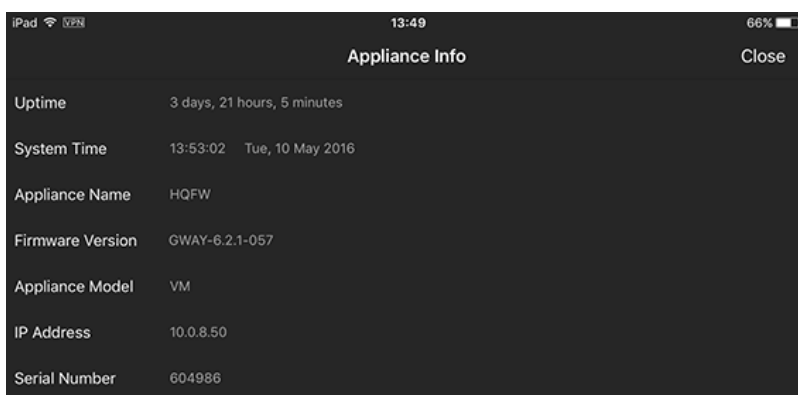
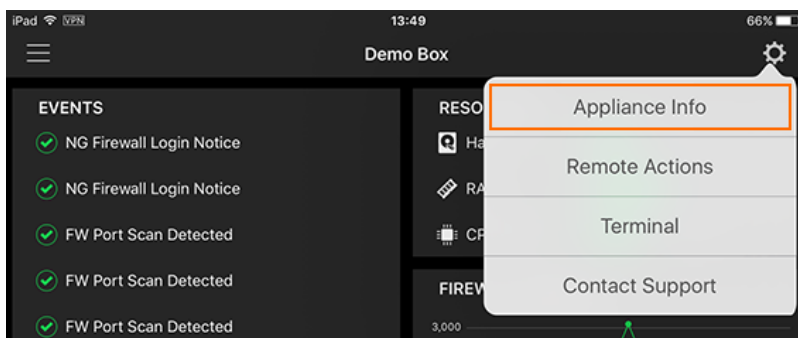
The status page offers the following features:

- **Events** – This section displays a list of recent events with a severity of warning and above.
- **Resources** – Provides general information on the unit's CPU and system status, such as memory and disk usage.
- **Overall Throughput (BIT/SEC)** – This section displays the overall traffic flow in bits per second.
- **Firewall Sessions** – Provides information on the number of allowed and blocked sessions and the unit's traffic throughput.

- **Dynamic Firewall Rules** – Displays all configured dynamic firewall rules with options to enable/disable or temporarily enable those rules.
- **Licenses** – Shows the licensing state of the unit.
- **Site to Site Tunnels** – Displays the status and details of TINA and IPsec VPN tunnels that are configured on the CloudGen Firewall.
- **Top Allowed Apps / Top Blocked Apps** – Shows the top applications that have been allowed or blocked during the last 24 hours by data size.
- **Top Allowed URL Categories / Top Blocked URL Categories** – Shows the URL categories that have been allowed or blocked, sorted by data/occurrences.
- **Top IPS Alerts** – Provides detailed information on alerts noticed by the Intrusion Prevention System (IPS) during the last 24 hours. For more information, see [Intrusion Prevention System \(IPS\)](#).
- **Top Malware Alerts** – Provides detailed information on malware detected by the firewall during the last 24 hours.

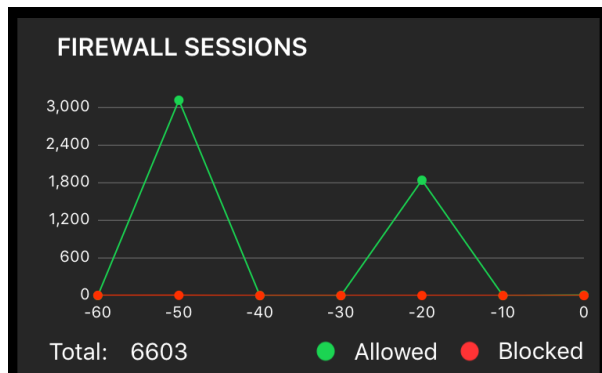
To view general information on the unit, such as uptime, system time, installed firmware version, license state, model, and serial number:

1. Tap the cogwheel icon on the top right of the status screen.
2. Select **Appliance Info** from the context menu.



View Status and Session Details

The firewall live view provides information on the number of allowed and blocked sessions and the unit's traffic throughput.



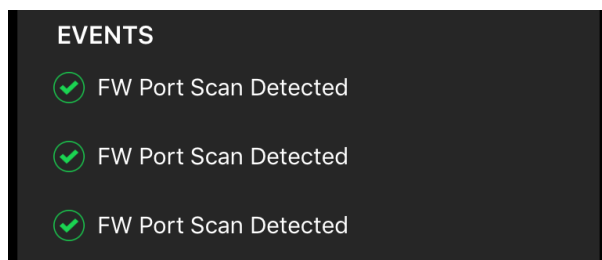
To view the dynamic graphs for allowed sessions, blocked sessions, and bit/sec throughput:

1. Open the status page of the firewall.
2. Tap **Firewall Sessions**.
3. Tap **Close** to go back to the status page.

To display the dynamic graphs for overall firewall traffic, tap **Overall Throughput (BIT/SEC)**. To view the graphs for box resource usage by memory, data disk usage, and system disk usage, tap **Resources**.

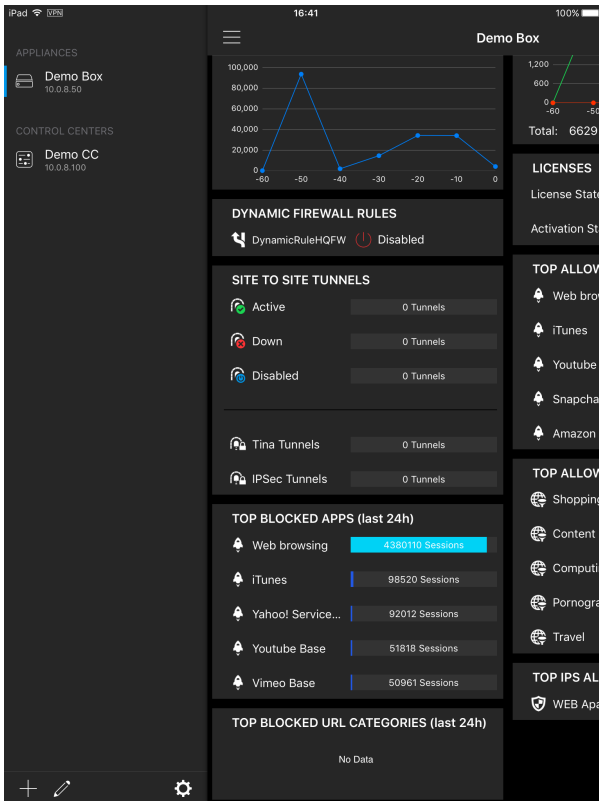
View Event Details

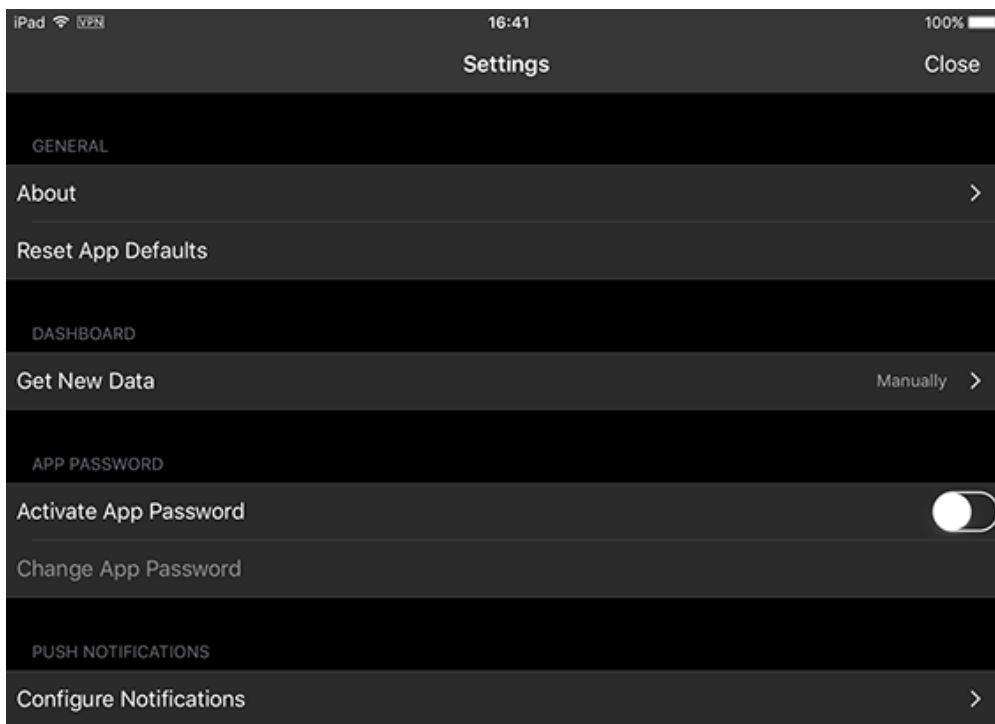
The **Events** section displays a list of recent events with a severity of warning and above. To access the list of events, tap **Events**. To view event details, tap the arrow icon on the right of the event.



Firewall Remote Control Settings

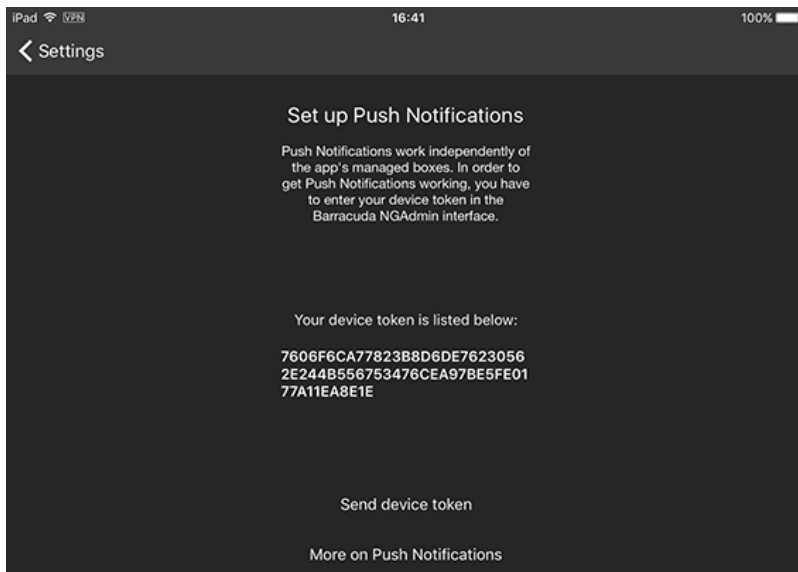
The Firewall Remote Control main menu provides a set of general options, allowing administrators to refresh the interface, change the Firewall Remote Control password, and configure notifications for managed firewall configuration changes. To access the **Settings** menu, tap the cog wheel icon at the bottom of the appliance list.





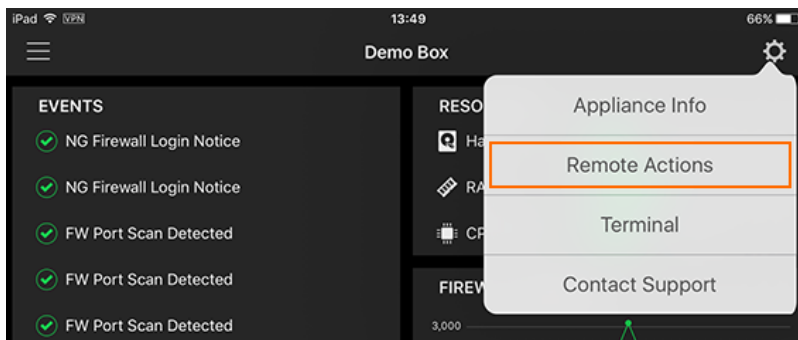
The **Settings** menu provides the following sections:

- **General** – This section displays the license agreement and provides general information on the product. To reset the Firewall Remote Control configuration to factory state, tap **Reset App Defaults**.
- **Dashboard** – Provides the option to refresh the configuration and update Firewall Remote Control with recent configuration changes on Control Center and managed firewalls. To update the configuration, tap **Get New Data**.
- **App password** – Offers the option to change the password for Firewall Remote Control.
- **Push notifications** – Tap **Configure Notifications** to get informed whenever the configuration on Control Center and / or managed firewalls is updated. To receive notifications, copy the device token that is displayed on the screen and paste it into your Firewall Admin interface. For more information, see [How to Configure Basic, Severity, and Notification Settings for Events](#).



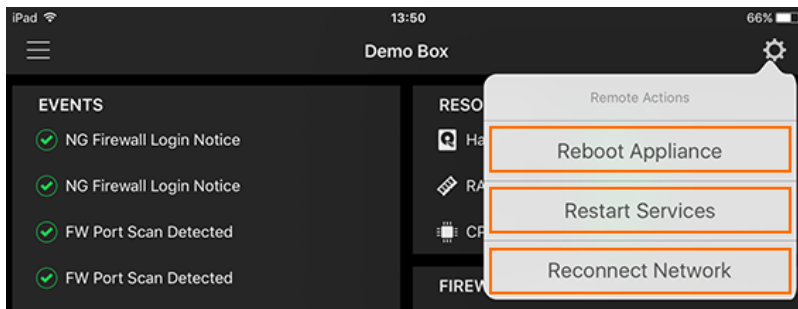
Perform Remote Actions

The Remote Actions feature allows system administrators to reboot the unit, restart all its services, reconnect the network, and rebuild management tunnels.



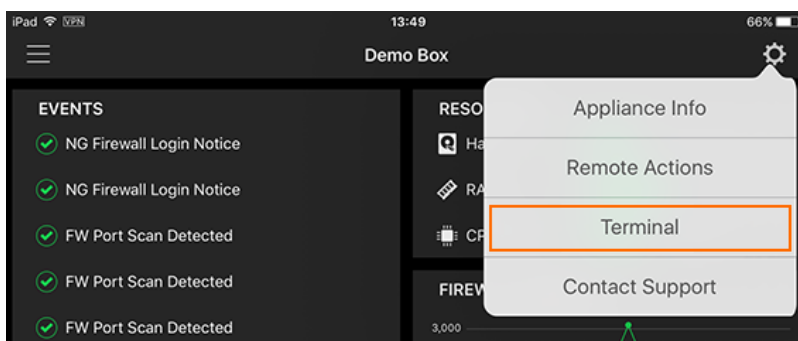
To perform a unit reboot, services restart, network reconnect, or management tunnel rebuild:

1. Tap the cogwheel icon on the top right of the status screen.
2. Select **Remote Actions** from the context menu.
3. Select the action to be performed.



Terminal Access

The **Terminal Access** section allows access to the Command Line Interface of a CloudGen Firewall or Control Center. This feature is not allowed on the Barracuda Networks demo units.

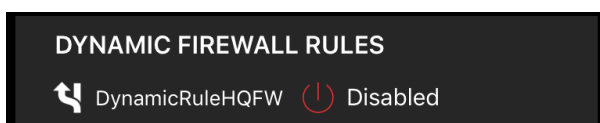


To access the command line via SSH:

1. Tap the cogwheel icon on the top right of the status screen.
2. Select **Terminal** from the context menu.

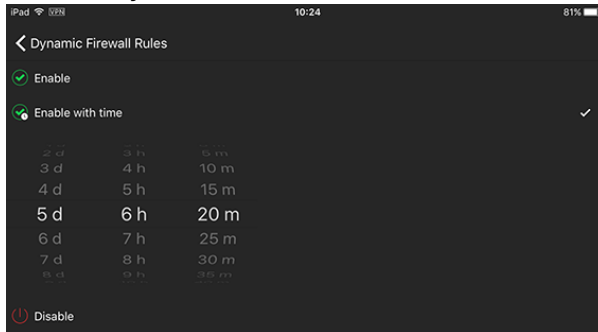
Dynamic Firewall Rules

Enable and disable dynamic firewall rules, for example, to provide a team with temporary access to a blocked web application.



1. Open the status page of the CloudGen Firewall.
2. Tap **Dynamic Firewall Rules** to display all configured dynamic firewall rules.

3. To enable or disable a rule, tap the arrow icon on the right of the rule.
 1. To enable the dynamic rule, tap **Enable**.
 2. To enable the dynamic rule for a specific time:
 1. Tap **Enable with time**.
 2. Select days, hours, and minutes for the rule to be enabled.



3. To disable the dynamic rule, tap **Disable**.
4. The rule is now enabled or disabled depending on the selected option.
5. To exit the dynamic rules screen, tap the back arrow icon.

Figures

1. connect.png
2. demo_cc_01.png
3. status_fw.png
4. appl_info00.png
5. appl_info.png
6. fw_sessions.png
7. events.png
8. rem_settings.png
9. settings01.png
10. push_notifications.png
11. remote_actions01.png
12. remote_actions.png
13. terminal01.png
14. dyn_rules.png
15. dyn_time.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.