

## How to Generate a System Report for Barracuda Networks Technical Support

<https://campus.barracuda.com/doc/79463392/>

When requested by Barracuda Networks Technical Support, a system report can be generated containing information on the firewall system and setup. The system report is saved as a tar archive (\*.tgz) on your firewall. The following information is included in the system report generated via Barracuda Firewall Admin:

Confidential data, such as passwords and keys, are not included in the system report unless you include a PAR file. Passwords and keys are included in PAR files.

- **Configuration Data** – System configuration information.
- **System Data** – Basic information about the system.
- **Service Data** – Information about introduced services and their configuration.
- **Version Information** – The currently installed version of the system.
- **Log Files** – All log files on the system.
- **Core Files** – Core files generated by the system.
- **Remove Core Files** – Remove core files generated by the system.
- **Statistics Files** – All statistics files on the system.
- **Access Cache** – A snapshot of the access cache's current state.
- **Operating System Data** – Information about the OS configuration.
- **Events** – All events on the system.
- **Configuration Archive (par)** – The system PAR file.
- **Kernel Dump Files** – Kernel dump files generated by the system.
- **Remove Kernel Dump Files** – Remove kernel dump files generated by the system.

System reports generated via command line contain the following information and files:

Name	Content	Comment
system-report.xml	The system report XML file. Contains all but statistics and log.	default
id_<num.num>	An identity file to distinguish between several system reports.	default
doit	A system report may be installed on a CloudGen Firewall as a hotfix. This script acts as the installer for the hotfix.	default
sysreport.xsl	The XML style sheet for the system report.	default
*.png	Image files for the system report.	default
statistics.tar.bz2	The statistics file collection as a bzip2-compressed tar archive. To view the content of the archive type: • tar -tvjf • statistics.tar.bz2	optional

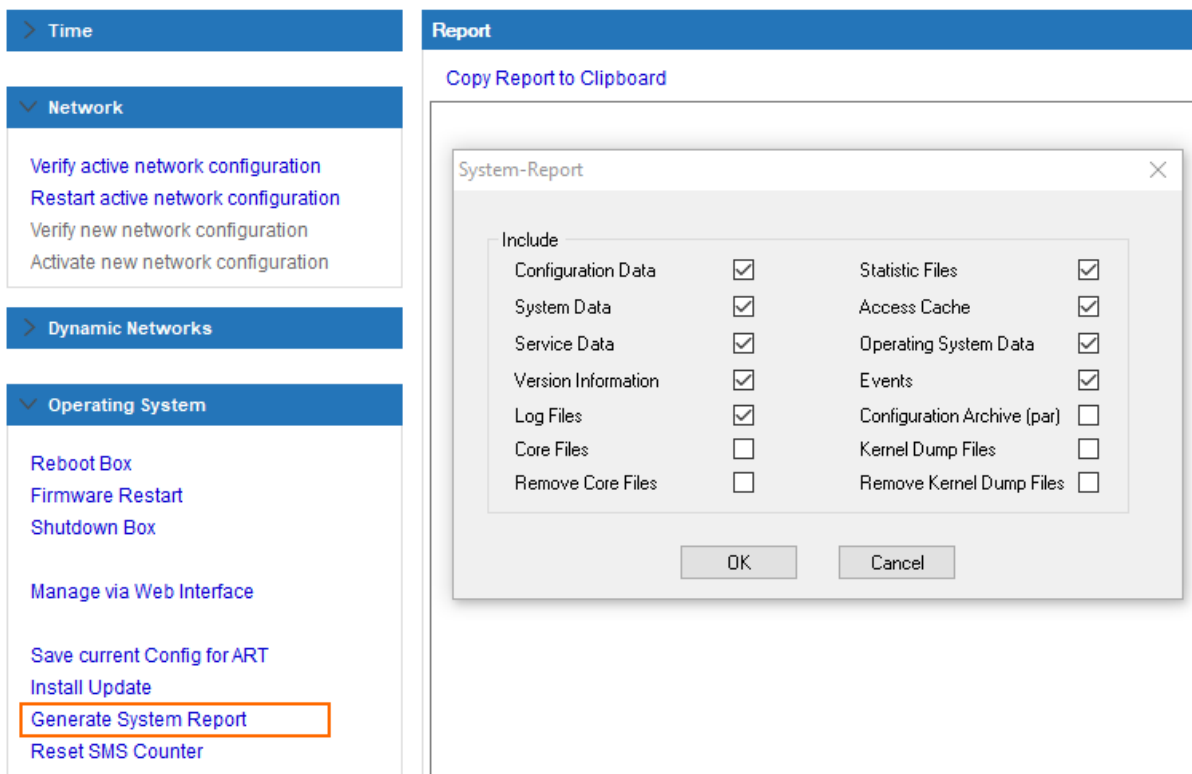
logs.tar.bz2	The log file collection as a bzip2- compressed tar archive. To view the content of the archive type: • tar -tvjf logs.tar.bz2	optional
box.pgz	The configuration archive	optional

## Create a System Report

A system report can be created using Barracuda Firewall Admin or via command line.

### Create a System Report Using Barracuda Firewall Admin

1. Log into the firewall.
2. Go to **CONTROL > Box**.
3. In the left menu, expand **Operating System** and click **Generate System Report**.



The screenshot shows the Barracuda Firewall Admin interface. On the left, the 'Operating System' menu is expanded, and 'Generate System Report' is highlighted with an orange box. On the right, the 'Report' section is visible, and a 'System-Report' dialog box is open. The dialog box has a title bar 'System-Report' and a close button. It contains a list of items to include in the report, each with a checkbox. The 'Include' section lists the following items:

Include	
Configuration Data	<input checked="" type="checkbox"/>
System Data	<input checked="" type="checkbox"/>
Service Data	<input checked="" type="checkbox"/>
Version Information	<input checked="" type="checkbox"/>
Log Files	<input checked="" type="checkbox"/>
Core Files	<input type="checkbox"/>
Remove Core Files	<input type="checkbox"/>
Statistic Files	<input checked="" type="checkbox"/>
Access Cache	<input checked="" type="checkbox"/>
Operating System Data	<input checked="" type="checkbox"/>
Events	<input checked="" type="checkbox"/>
Configuration Archive (par)	<input type="checkbox"/>
Kernel Dump Files	<input type="checkbox"/>
Remove Kernel Dump Files	<input type="checkbox"/>

At the bottom of the dialog box are 'OK' and 'Cancel' buttons.

4. In the **System Report** window, select the data that you want to include in the report, and click **OK**.
5. In the **Save As** window, select where you want to save the system report tar archive (\*.tgz) file. A **Progress** window opens after you make your selections.

You can now email the system report file to Barracuda Networks Technical Support.

### Create a System Report via Command Line Interface

The name of the executable is system-report and is located in: /opt/phion/bin/

1. Log into the firewall via SSH or serial console.
2. Create a system report:
  - Standard system report:

```
/system-report
```

- Custom system report:

```
/system-report --collect <comma separated list of parameters - see list below>
```

Available command line parameters E.g., /system-report --collect  
config, services, log, event

Parameter	Description
config	<ul style="list-style-type: none"><li>• Authentication Schemes</li><li>• Administrative Settings</li><li>• Watchdog</li><li>• System Settings</li><li>• Control Settings</li><li>• Firewall Settings</li></ul>
services	Service data
system	System data
versions	Version information
log	Log data
stat	Statistics data
accesscache	Content of the access cache
phionos	Barracuda CloudGen Firewall information
event	Event data
all	Collects all available data except the par file. To exclude data, add one of the parameters above with a leading no.

Both commands generate a system report that contains config, service, log, and event data.

### PAR File Integration

By default, a system report does not contain a PAR file; however, it is possible to integrate a PAR file into a system report.

To include a PAR file into a system report, type:

- `/system-report --par`

A system report is a gzip-packed tar archive (\*.tgz) and can be viewed within the command-line interface.

To view the content of a system report type:

- `tar -tvzf system-report.tgz`

## Viewing System Reports

---

Statistics and log files are only viewable with the aid of the statistics or log viewer of Barracuda Firewall Admin. Therefore, system reports can be installed on a firewall. System reports are designed as hotfixes and can simply be installed like any other hotfix. When installing a system report, the files `system-report.xml`, `sysreport.xsl`, and the required images will be loaded into the firewall's internal web server in order to be viewable by a web browser.

### Step 1. Configure the Internal Web Server

Before installing system reports, verify that **Enable System Reports** is selected in the forwarding firewall settings. This step is required to view the content of the report.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Settings**.
2. In the left menu, select **Authentication**.
3. Click **Lock**.
4. In the **Authentication Server Configuration** section, click **Show/Edit** next to **Operational Settings**. The **Operational Settings** window opens.
5. In the **CGI Interface** section, set **Enable System Reports** to **Yes**.
6. Click **Send Changes** and **Activate**.

After changing these settings, a firmware restart (**CONTROL > Box**) is required.

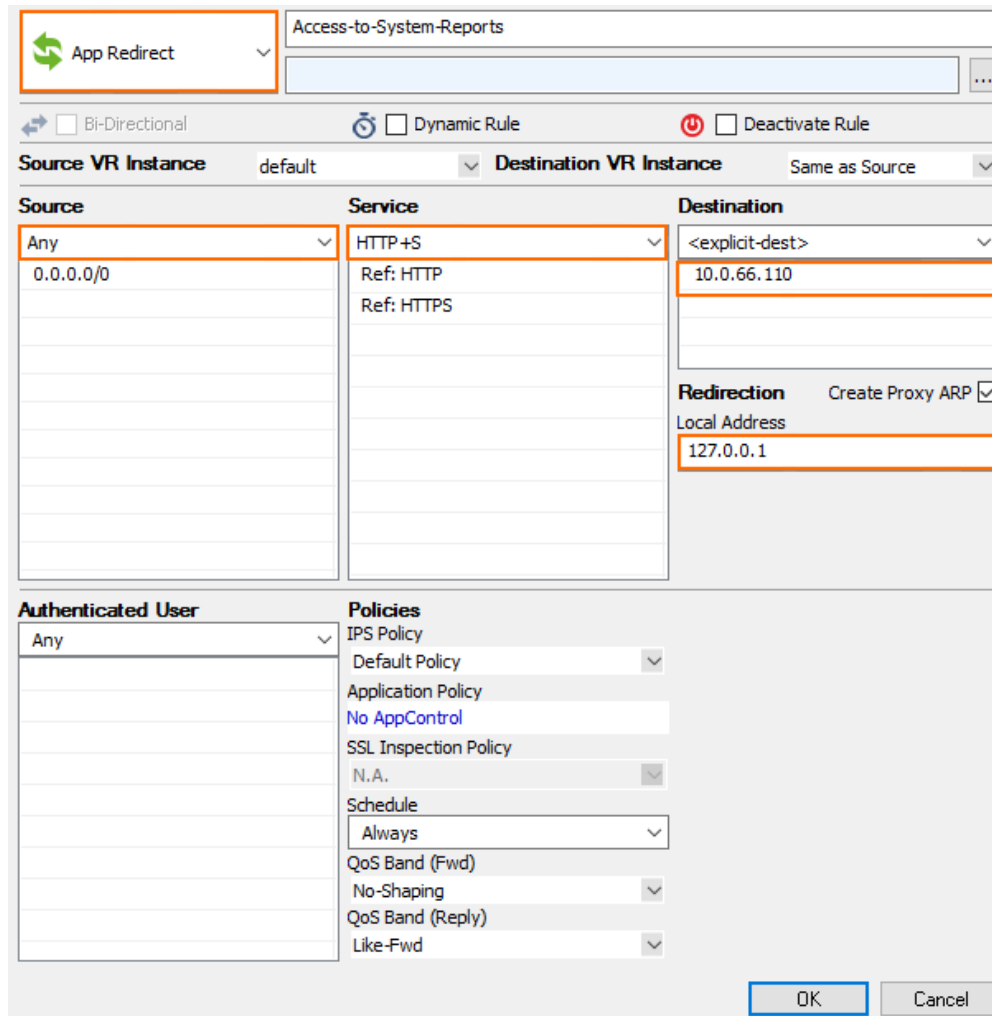
### Step 2. Configure the Firewall

To be able to view statistics and log data with a web browser, an access rule must be introduced. This is necessary because, due to security reasons, the integrated web server only listens for connections on the loopback interface.

### Viewing System Reports via Web Browser

Create a rule with the following settings:

- **Action - Local Redirect**
- **Source** - Define the desired source network
- **Service - HTTP+S**
- **Destination** - The box IP address of the firewall
- **Redirection** - The loopback address 127.0.0.1



The screenshot shows the configuration window for an "App Redirect" rule. The rule name is "Access-to-System-Reports". The "Source VR Instance" is set to "default" and the "Destination VR Instance" is set to "Same as Source". The "Source" field is set to "Any" (0.0.0.0/0). The "Service" is set to "HTTP+S" (Ref: HTTP, Ref: HTTPS). The "Destination" is set to "<explicit-dest>" (10.0.66.110). The "Redirection" section is checked, and the "Local Address" is set to "127.0.0.1". The "Authenticated User" is set to "Any". The "Policies" section includes: IPS Policy (Default Policy), Application Policy (No AppControl), SSL Inspection Policy (N.A.), Schedule (Always), QoS Band (Fwd) (No-Shaping), and QoS Band (Reply) (Like-Fwd). The "OK" and "Cancel" buttons are at the bottom right.

Source	Service	Destination
Any 0.0.0.0/0	HTTP+S Ref: HTTP Ref: HTTPS	<explicit-dest> 10.0.66.110

**Redirection** Create Proxy ARP ☒  
Local Address  
127.0.0.1

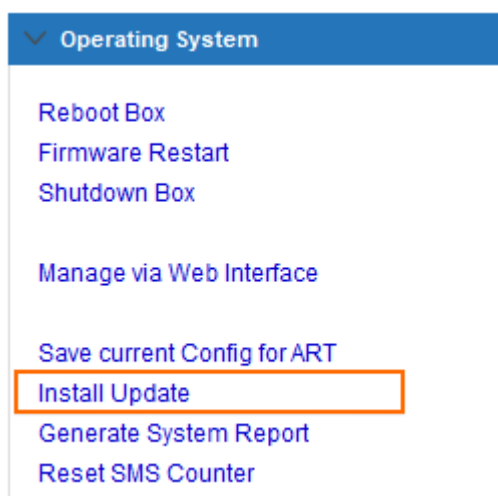
**Authenticated User**  
Any

**Policies**  
IPS Policy  
Default Policy  
Application Policy  
No AppControl  
SSL Inspection Policy  
N.A.  
Schedule  
Always  
QoS Band (Fwd)  
No-Shaping  
QoS Band (Reply)  
Like-Fwd

OK Cancel

### Step 3. Install the System Report


1. Log into the firewall.
2. Go to **CONTROL > Box**.
3. Click **Install Update**, and specify the source of the desired system report.



4. Install the system report.

To view previously created system reports, open a web browser to the following URL:  
<http://<ip>/cgi-bin/show-sysreports>

Note that <ip> stands for the IP address or a DNS-resolvable name of the configured firewall.


**CloudGen Firewall System Report**
---/fd-test

Base
Servers
Routing
FW History
ACPF/KTINA
Config
OS
Top
CPU-Time
Netstat
Events

**System**

Base Version	GWAY-7.2.0-303.nightbuild	
Time	2017:04:21 13:19:02	
Domain join status	Join NOT ok	
Boxname	fd-test	
FQDN	---/fd-test	
CC IP Address	single-box	
Appliance Hardware	VM	
Virtualisation Method	VMWare	
Virtualisation Sub-Method		
Serial	None	
CompactFlash	no	
Write stat	yes	
Demo-Mode	yes	
Export-Mode	no	
Compression	no	
HW-Crypt	no	
Padlock	no	
VPN-Shaping	no	
SME	no	
SME-MC	no	

---

**Installed Hotfixes**

---

**Box services**

boxconfig		up
bsms		up
psyslog		up
dist		up
log		up
bsyslog		up
phibs		up
bsnmp		up
control		up
restd		up
logwrap		up
qstat		up
bdns		up

## Viewing Statistics

Statistics data of installed system reports can be viewed within the statistics viewer of Barracuda Firewall Admin. For more information, see [STATISTICS Tab](#).

## Viewing Log Files

Viewing log files is only possible if a special registry key was set at the client workstation the Barracuda Firewall Admin client is running on.

1. Start the Windows Registry Editor by typing `regedit` in the MS Windows command line.

2. Navigate to HKEY\_CURRENT\_USER\Software\Barracuda\ngadmin\log
3. Right-click and choose **New** followed by **DWORD Value**.
4. Set the name of the registry key to showrange and its value to 1Viewing System Reports

Log data of installed system reports can be viewed within the log viewer of Barracuda Firewall Admin. For more information, see [LOGS Tab](#).

## Uninstalling System Reports

---

System reports can be removed via the web interface or directly on the CLI.

1. Inside the web interface, each system report has a **Remove** button.
2. Within the command line interface, type:
  - `/var/phion/fwauthd/cgi-bin/remove-sysreport -r <id>` where <id> stands for the system report id.

When removing a system report, all of its data will be removed from the system and no additional warning message is displayed.



## Figures

1. report\_01.png
2. reports\_rule.png
3. install\_update.png
4. sys\_report\_01.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.