Step 5 - Verify Scheduled Reports Migrated from Connected Devices to Vx

https://campus.barracuda.com/doc/84968186/

This step is needed if you have connected one or more of the following devices:

- Barracuda Web Security Gateway
- Barracuda Web Application Firewall

When you first connect one or more Barracuda Web Security Gateway or Barracuda Web Application Firewall devices to the Barracuda Reporting Server, your scheduled reports in the connected devices are automatically migrated to the Barracuda Reporting Server.

The migration process begins when you enter the Barracuda Reporting Server connection information within the connected device.

- Refer to Reporting with the Barracuda Reporting Server in the Barracuda Web Security Gateway documentation for details.
- Refer to How to Configure Syslog and Other Logs in the Barracuda Web Application Firewall documentation for details

All information on connected devices remains on those devices, even after they are connected to the Barracuda Reporting Server. Reports created with the Barracuda Reporting Server include data from the time the report is migrated to the Barracuda Reporting Server. Historical data, gathered by the device before its connection to the Barracuda Reporting Server, are not migrated to the Barracuda Reporting Server. If the device is disconnected from the Barracuda Reporting Server, either intentionally or unintentionally, then data will be missing from that period of time. If you intentionally disconnected the device, that data will not be sent to the Barracuda Reporting Server. If there was an unintentional connection error, connected devices will store the data and continually attempt to resend it to the Barracuda Reporting Server.

Step 1: Viewing Migrated Reports

To complete the migration process:

1. In the Barracuda Reporting Server, navigate to the **BASIC > Administration** page.
2. In the **Connected Devices** section, locate the newly connected device and click **View Migrated Reports**.
3. The **Migrated Scheduled Reports** dialog appears. It displays the **Report Name**, **Frequency**, and **Time Frame** to help you identify the reports. The **Migration Status** column shows whether the report was migrated successfully. Occasionally, errors occur during migration.

4. For reports showing an error, click **View Details** to see the issues with migrating that report.

No Migrated Reports

The are some cases in which the Migrated Scheduled Reports dialog might not display any reports. A message informs you why there are no reports to display.

For details, refer to Troubleshooting.

Step 2: Verifying and Enabling Migrated Reports

After migration is complete, you must enable the migrated reports. This is an opportunity to double-check the report information for errors before the reports are generated.

To enable migrated reports:

1. Navigate to the **REPORTS** page for the targeted connected device.
2. In the **Scheduled Reports** section at the bottom of the page, locate a newly migrated report. It will display as **Disabled**.
3. Click **Edit** for the migrated report. Scroll to the top of the page and verify that the information is correct for the migrated reports.
4. In the **Schedule Report** section, select **Enabled**, then click **Save Changes** in the top right corner.
   In the **Scheduled Reports** section, the report appears with the status of **Enabled**.

Disconnecting Devices and Associated Reports

If you choose to disconnect a device from the Barracuda Reporting Server, the reports you originally created on the connected device are re-enabled with their original settings. You can again manage reports within the Barracuda Web Security Gateway or Barracuda Web Application Firewall. Any updates you might have made to those original reports, or any new reports you created in Barracuda Reporting Server, are not migrated back to the disconnected device.

If you choose to disconnect a device, reports created or migrated to the Barracuda Reporting Server, and report modifications made within Barracuda Reporting Server, remain within the Barracuda Reporting Server and can continue to be managed there.

Barracuda Web Application Firewall Report Exceptions

The following reports must be viewed and managed through the Barracuda Web Application Firewall. These reports are not migrated to the Barracuda Reporting Server. When you look at migrated scheduled reports for the Barracuda Web Application Firewall, a message appears, informing you that these reports were not migrated.

Reports that must be viewed and managed in the Barracuda Web Application Firewall:

PCI DSS Reports

- PCI Attacks
- PCI Compliance (PCI DSS v3.1)

Administration/Audit Reports

- Server Monitoring
- RBA Activity

Config Summary

- Application Summary
- Certificate Status Report
- Administrative Accounts
- URL Profile and ACLs Summary
- Server Summary
- Exception List

System Summary Reports:

- CPU UtilizationShow Report
- Memory UtilizationShow Report
- Total Bandwidth