Resolved and known issues

Topic 70198 | Release Notes | IQ-Series Appliance | Updated: 31-Mar-2016

Applies to:	Forcepoint IQ-Series appliance v1.6, 1.6.1

Resolved issues

The following issues have been resolved since the release of the Websense IQ-Series appliance version 1.6.0:

- Frequent erroneous Linux swap space high usage alerts appeared.
- Authentication session timeout duration was always 1 day, regardless of the value set in the cloud portal.
- The traffic monitor set_default_display command did not set monitor display attributes as expected.
- In some cases, a license expiration alert message did not appear as expected.
- Incorrect error message appeared during connection to an Active Directory server.

Known issues

The following issues are known to exist for the Forcepoint IQ-Series appliance version 1.6.1:

Only IP address-to-policy mapping is supported.

Users of an appliance must be assigned to a policy that has been mapped to that appliance. When a user is assigned to a policy that is not mapped to an appliance, and appliance policies require user authentication, the authentication operation fails.

No workaround

Web traffic monitor does not support a colon (":") as part of an FTP username.

No workaround

Web traffic monitor does not support the display of a custom category description.

"Custom" appears in the category field instead.

No workaround

Google Quick UDP Internet Connections (QUIC) protocol is not supported.

This experimental protocol should be disabled.

Workarounds:

To disable Google QUIC in the browser:

1. Enter the following URL in the Chrome browser address bar:

   `chrome://flags/#enable-quic`
2. Select **Disabled** in the drop-down list that appears below the heading "Experimental QUIC protocol. Mac, Windows, Linux, Chrome OP, Android."
3. Click **Relaunch now** at the bottom of the page.
4. To verify that the protocol is disabled:
   a. Enter the following URL in the Chrome browser address bar:

      `chrome://net-internals/#quic`
   b. Verify that the following entry appears:

      `QUIC Enabled: false`

As an alternative, you can disable Google QUIC in the network as follows:

1. Create a new custom protocol in the Add Protocol page named, for example, "Google QUIC."
2. In the Add Protocol Identifier dialog box:
   - Assign the new protocol to ports 80 and 443.
   - Specify its transport method as **UDP**.
3. Click **OK** and **Save**.
4. Set the disposition of the newly created protocol to **Block**.

In some cases, the cloud service Google redirect feature does not work properly when processing i-Series appliance traffic.

Google redirect is not supported:

- When session-based authentication is used
- When Google does not automatically change the URL to an https address

See the Release Notes for Websense Cloud Web Protection Solutions for details about this feature.

NTLM2 Session authentication is not supported.

Workaround:

Use either NTLMv1 or NTLMv2 authentication.

- **Please contact Forcepoint Technical Support to configure your appliance to force the use of NTLMv1 on specific browsers.**
- **If you are using Mozilla Firefox, you can perform the following steps to configure the browser to use NTLMv1 authentication:**
  1. Open the Firefox browser and enter the following in the address bar:

     `about:config`
  2. Enter the following in the Search field:

     `network.auth.force-generic-ntlm-v1`

3. Double-click the entry and verify that the status changes to:

   `user set`

4. Enter the following in the Search field:

   `network.automatic-ntlm-auth.trusted-urls`

5. Enter the appliance IP address.

- **Use the following Windows-specific resolution to configure your browser to use NTLMv2.**

  1. Open the Windows Control Panel on your computer and select **Administrative Tools**.
  2. Double-click **Local Security Policy** to open the Local Security Policy window.
  3. In the Local Security Policy window left pane, navigate to **Security Settings > Local Policies > Security Options**.
  4. In the Local Security Policy window right pane, double-click **Network security: LAN Manager authentication level** to open the Network security: LAN Manager authentication level properties dialog box.
  5. Select **Send NTLMv2 response only. Refuse LM & NTLM** from the drop-down list.
  6. Click **Apply**.
  7. Click **Yes** in the confirmation dialog box.

Email address as a username for Active Directory validation from some browsers is not supported.

Workaround:

Use the domain\username format for user authentication.

Upgrade status may display as “Failed” after a successful upgrade.

Refreshing the appliance user interface immediately after the upgrade operation may cause incorrect error message displays.

Workaround:

Please wait approximately 5 minutes to refresh the user interface after the upgrade.

If the problem persists for longer than 5 minutes, please contact Forcepoint Technical Support.

ICQ client traffic is not supported via port 443.

ICQ client connections are not allowed, even when the relevant protocol and category for ICQ traffic are allowed.

Workarounds:

One of 2 options is available:

- Define the ICQ server as a trusted destination in the Forcepoint blueSKY portal (Network Devices appliance **Networking** tab).

- If the ICQ client includes port change support, switch to a port other than 443, ensuring that the port is not otherwise blocked by the appliance or a network firewall.

The Forcepoint blueSKY Security Gateway transparent proxy does not work properly when located adjacent to an explicit proxy in a network.

One of 2 results occurs, depending on proxy location:

- If the explicit proxy is located between the client and the transparent proxy, then the transparent proxy's user identification process does not work. This deployment should be avoided.
- If the transparent proxy is located between the client and the explicit proxy, the authentication process cannot complete.

Workaround:

To resolve the second bullet issue above, include the appliance IP address in the individual browser's non-proxied destination list.

You can also disable the explicit proxy to allow the authentication process to complete.

The appliance may be difficult to register after it has first been deleted from the appliance list and then added again.

Workaround:

Contact Forcepoint Technical Support for a workaround.

Multiple users can log on to the same server and be allowed to browse using another logged-on user's policy.

Workaround:

Use the session-based authentication method.

A user may be allowed to transmit non-Web traffic before being authenticated for Web requests if the source IP address for the server is currently mapped to a different user.

No workaround

Google Chrome and Mozilla Firefox do not support the Forcepoint blueSKY Copy to Clipboard function.

No workaround

Web sites that use AJAX may display unexpected results when handling a Forcepoint blueSKY block page (Quota or Confirmation).

No workaround

User Quota or Confirmation status may not be synchronized with the appliance when SSL traffic is routed to the Forcepoint blueSKY portal.

If the Forcepoint blueSKY portal initiates a block page for an SSL traffic request, the cloud portal cannot update the appliance regarding the request status. The result is that Quota or Confirmation pages and time frames may not be aligned with the configured time frame parameters.

No workaround

Confirm page may appear embedded in a target site's web page.

No workaround

Custom block page notifications (confirm/quota/authentication) for the appliance and the cloud portal exhibit some display differences.

- Users with no web access permission receive a browser error rather than a block page when they tries to access an HTTPS web site
- A custom page configured with a language other than English is supported, but multiple language configuration for a single page is not supported.

  However, this language limitation does not apply if you are using session-based authentication.

No workaround

Block pages may not be displayed as expected after the confirmation timeout expires for some SSL traffic requests.

Workaround:

Reopen the Web page to generate a new browsing session.

An HTTPS site request generates a continuous loop of Quota/Confirm page displays

Clicking **OK** only generates another Quota/Confirm page, with no access to the site.

This situation may occur when the appliance is configured to redirect SSL traffic to the cloud, and an appliance quota session for the same category has just expired.

Workaround:

Define a custom category for desired HTTPS sites and configure a Quota/Confirm action for the category.

Multiple simultaneous connections to the cloud portal may generate multiple Quota/Confirm page displays

Workaround:

Click **OK** on each Quota/Confirm page until the desired web site appears.

Continuous Quota/Confirm pages appear after a No Content HTTP error is received.

This situation occurs when policy dictates that block and notification messages are not decrypted. The SSL connection ends, and the browser displays the last page you were served (i.e., the Quota/Confirm page).

No workaround

Some SSL web sites are not correctly blocked when SSL decryption for block pages is disabled.

Workaround:

Perform 1 of the following actions:

- Enable SSL decryption in the cloud portal (**Policy > SSL Decryption**)
- Ensure that client web browsers support TLS v1.0 and later and that TLS 1.0 is enabled.

User authentication based on category may be unsuccessful.

This situation occurs when the authentication prompt is received from the cloud service rather than the appliance.

No workaround

Authentication bypass for non-ASCII URLs or user agents is not supported.

No workaround

Google Chrome may block certain HTTPS sites to which it has pinned a certificate.

Workarounds:

- Import the Forcepoint blueSKY Security Gateway default certificate to Chrome's CA storage location. (recommended)
- Use a browser other than Chrome. You will receive a warning message that allows you to click through and access the site.

The appliance does not detect NFS UDP packets and they are not processed.

TCP packets are correctly detected and processed.

No workaround

The appliance does not support oversized, non-standard frames (greater than 1500 bytes) for protocol detection.

Data transferred in these large frames is not processed by the appliance.

No workaround

Mobile traffic monitoring may not be supported.

Workarounds:

- Bypass traffic from WiFi networks that carry mobile traffic.
- Use the authentication bypass capability to designate the internal IP address/range for a network that hosts mobile clients, to avoid authentication on that network.

You might consider testing mobile traffic monitoring first and enabling the monitoring capability gradually in the Forcepoint blueSKY portal.

Creating protocol exception definitions that are identical except for the exception action should be avoided.

No workaround

A custom category that includes an HTTPS URL defined with a full path is not supported.

Destination IP address or a hostname for an HTTPS site are valid parameters.

Workaround:

Use session-based authentication.

Incorrect screen may appear when the appliance cannot handle Java script properly.

No workaround

Clicking the "x" icon in an appliance pop-up alert may not close the window.

Workaround:

Click the **Close** button in the pop-up window.

A Google Chrome browser may display the "Who are you?" page after briefly displaying an authentication dialog box.

Workarounds:

- Click 1 of the following buttons to return to the authentication dialog box from the "Who are you?" page:
  - **Login** (if you have already registered your email address for Internet access)
  - **Register** (if you have not yet registered your email address)
- To avoid this issue, you can modify Chrome's advanced settings:
  1. In the Chrome browser menu, select **Settings**.
  2. Click **Show advanced settings**.
  3. In the Privacy section, clear the **Use a prediction service to help complete searches and URLs typed in the address bar** check box.

Having more than 8 certificates in a chain may cause browsing problems in Google Chrome.

No workaround

Google Chrome web store applications cannot be installed if you are using session-based authentication.

Workaround:

Click here for details.

A broken certificate chain may be rejected by the appliance but cause no visible error message in the cloud portal.

Unknown CA alerts may result from this situation.

Workaround:

Verify that your certificate chain is successfully uploaded.

Connectivity with appliance may be lost after changing the VLAN tag while connected to the appliance management interface.

Workaround:

Ensure that your client routing includes the new VLAN configuration to recover the connection.

Requests for the YouTube education page are not supported for SSL if SSL decryption for the category is not enabled.

This limitation does not apply when session-based authentication is used.

No workaround