

# Resolved and known issues

Topic 70044 | Release Notes | IQ-Series Appliance | Updated: 15-Nov-2013

<b>Applies to:</b>	Websense IQ-Series appliance v1.1
--------------------	-----------------------------------

## Resolved issues

---

The following issues have been resolved since the release of the Websense IQ-Series appliance v1.0:

**A user can now block appliance management access through the bridge interface.**

**Custom block pages cannot be defined and configured in the Websense blueSKY portal. Only the default block page template can be used.**

**Default block page notifications for the appliance are different from those displayed for Websense blueSKY.**

**The SPDY protocol is not supported.**

**Facebook is filtered as Social Networking rather than Society & Lifestyles, as it is listed.**

## Known issues

---

The following issues are known to exist for the Websense IQ-Series appliance:

**On the Configuration > Upgrade Management page, clicking a download or install upgrade icon does not change the Status column value for this item.**

Workaround:

Click F5 to refresh the page.

If a “Failed” status appears after a page refresh, please wait a few minutes, until the appliance restarts, and check the status again.

**The Websense 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 use of VLAN tags is not supported.**

Workaround:

Locate the appliance in an area of your network that does not use VLANs.

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

Workaround:

1. Stop the cloud communication service using the following command:  
`/etc/init.d/tsaas-platty stop`
2. Delete the config directory:  
`rm -rf /opt/websense/platty/config/*`
3. Start the cloud communication service using the following command:  
`/etc/init.d/tsaas-platty start`
4. Register the appliance.

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

No workaround

**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

**A Hebrew policy name may not be displayed correctly in a Websense blueSKY report's Detailed Summary table.**

No workaround

**Invalid time zone values in the Websense blueSKY portal may not be correctly interpreted by the appliance manager.**

Workaround:

Use the appropriate local time zone in the appliance manager or contact Websense Technical Support for a workaround.

**Appliance alert format and phrasing may not be clear.**

These alerts are only for Websense Technical Support representatives. You may disregard them.

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

No workaround

**Web sites that use AJAX may display unexpected results when handling a Websense 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 Websense blueSKY portal.**

If the Websense blueSKY cloud 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

**When multiple browser tabs are open to a Quota/Confirm page, and Confirm is clicked for 1 tab, the confirm code token is added to the second site's URL.**

Workaround:

Close the second tab and access the site via its original URL.

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

Workaround:

Refresh the web page.

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

- ◆ Only the header and graphic at the top of the appliance notification may be customized. Other custom text changes in a notification do not display properly.
- ◆ 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. However, multiple language configuration for a single page is not supported.

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.

**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 Websense 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.**

Workaround:

Bypass traffic from WiFi networks that carry mobile traffic.

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

**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.

No workaround

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

No workaround

**Appliance upgrade description does not appear in the cloud portal Upgrade Management table.**

Workaround:

Find the upgrade description in the appliance **Configuration > Upgrade Management** page.

**Adding a user-defined protocol does not succeed on the first attempt.**

Subsequent attempts to add the custom protocol are allowed.

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.

**The upgrade log file is not available on the appliance Configuration > Upgrade Management page, in the Upgrade History table.**

No workaround

**In Microsoft Internet Explorer, a user may not be directed to an HTTPS web site target after clicking to accept the Confirm/Quota request.**

Workaround:

Click twice to accept the Confirm/Quota request.

**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.

**A broken certificate chain may be rejected with no visible error message.**

“Unknown CA” warnings may result from this situation.

Workaround:

Verify that your certificate chain is successfully uploaded.

