Known issues

Topic 70033 | Release Notes | Websense blueSKY Security Gateway | Updated: 02-July-2013

Applies to:	Websense blueSKY Security Gateway IQ-Series appliance v1.0

The following issues are known to exist for Websense blueSKY Security Gateway:

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.

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 user may access the appliance via the bridge (B2) port.

Please contact Websense Technical Support for a 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

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

No workaround

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

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

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

No workaround

A Websense blueSKY form-based authentication page may be slow to display for some HTTPS Web sites.

This issue may occur with an HTTPS site that has a slow TLS “handshake” process.

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 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

The SPDY protocol is not supported.

No workaround.

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

The category update to change this categorization is pending.

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