

Release Notes for Websense IQ-Series Appliances

Topic 70114 | Release Notes | IQ-Series Appliance | Updated: 31-Oct-2014

Applies to:	Websense IQ-Series appliance v1.3, 1.3.1, 1.3.2
--------------------	---

Contents

- ◆ [Version 1.3.2 release update](#)
- ◆ [Version 1.3.1 release update](#)
- ◆ [New version 1.3 product features](#)
- ◆ [Installation and upgrade](#)
- ◆ [Resolved and known issues](#)

The Websense IQ-Series appliance is a component of Websense blueSKY Security Gateway, a Web security solution that provides on-premises URL analysis and application/protocol detection for Web traffic, along with centralized policy management and reporting capabilities in the cloud. The appliance [Quick Start Guide](#) illustrates the ease with which this Web security solution can be implemented.

The IQ-Series appliance hosts the Websense URL category master database, allowing the efficient analysis of web site request URLs. The appliance also provides protocol detection capabilities and policy enforcement.

When analysis indicates that a web request requires further examination, the appliance transparently routes that traffic to the cloud, where Websense blueSKY Security Gateway analytics are applied and policy is enforced. Management of on-premises appliances is also performed in the cloud.

View detailed product user information in the following Help systems:

- ◆ [Websense IQ-Series Appliance Help](#)
- ◆ [Websense blueSKY Security Gateway Help](#)

Use these Release Notes to learn about version 1.3 product features, release updates for versions 1.3.1 and 1.3.2, installation and upgrade tips, and resolved and known issues lists.

Version 1.3.2 release update

Applies to:	Websense IQ-Series appliance v1.3, 1.3.1, 1.3.2
--------------------	---

This release of the Websense IQ-Series appliance addressed the following issue:

SSL vulnerability (POODLE)

The critical SSLv3 vulnerability that affects the Websense IQ-Series appliance has been identified in CVE-2014-3566.

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. TLS (Transport Layer Security) has since superseded SSL. However, support for the older SSL version 3.0 still exists in the majority of applications and can therefore lead to software (such as browsers) being forced into using a vulnerable SSLv3 connection.

The vulnerability can be exploited by inducing a client's browser into making multiple browser requests over HTTPS with SSLv3, and inferring details about the encrypted contents that allow an attacker to compromise the security of SSLv3.

Version 1.3.1 release update

Applies to:	Websense IQ-Series appliance v1.3, 1.3.1, 1.3.2
--------------------	---

The version 1.3.1 release of the Websense IQ-Series appliance, which is included in version 1.3.2, addressed the following issues:

◆ **Bash vulnerabilities (Shellshock)**

The critical Bash vulnerabilities were first identified in CVE-2014-6271. Subsequent investigation of the Bash code revealed other, related vulnerabilities.

The vulnerabilities present in Bash (Bourne Again Shell) up to version 4.3 can be exploited by malicious persons, including over HTTP.

Bash is a shell program found in a range of Unix-based operating systems such as Linux and Mac OS X. The original vulnerability (CVE-2014-6271) allows for remote execution of arbitrary commands via crafted environment variables, which can be exploited in a number of ways. Most Linux and Unix-based systems are vulnerable, because the Bash shell is one of the most common installs on a Linux system and is widely used.

Many programs like SSH, telnet, and CGI scripts allow Bash to run in the background, allowing the vulnerability to be exploited remotely over the network, which makes this a very serious issue.

Appliance version 1.3.1 includes a new version of the Bash program that has been corrected to eliminate these vulnerabilities.

◆ **SSL/TLS sites were not loading properly for session-based clients**

Some SSL/TLS sites (e.g., Facebook) did not load successfully from some browsers (e.g., Firefox running on Linux) due to issues with faked certificate generation by the device's SSL/TLS engine, resulting in a man-in-the-middle problem.

New version 1.3 product features

Topic 70117 | Release Notes | IQ-Series Appliance | Updated: 31-Oct-2014

Applies to:	Websense IQ-Series appliance v1.3, 1.3.1, 1.3.2
--------------------	---

This version of Websense blueSKY Security Gateway contains new features and fixes. This section of the Release Notes describes the new features that appear in the cloud portal in association with this release of the Websense IQ-Series appliance:

- ◆ *[Session-based authentication](#)*
- ◆ *[Authentication bypass for internal networks](#)*
- ◆ *[Authentication decryption bypass for appliances](#)*

See the [Websense blueSKY Security Gateway Release Notes](#) for updates on Websense blueSKY portal changes.

Session-based authentication

This release now supports session-based authentication for traffic that is routed through an IQ-Series appliance. This capability allows the appliance to authenticate users in a thin client network who share the same IP address. In session-based authentication, a cookie is injected into the web traffic and analyzed by the appliance to ensure the request is from a valid user.

Network addresses and IP address ranges that you want to use session-based authentication are configured in the Websense blueSKY portal, in the Network Devices appliance Authentication tab. Session length is also defined on this tab, in the Session Timeout section.

Client web browsers must support TLS v1.0 and later. TLS 1.0 must be enabled.

Some web browsers require special configuration when session-based authentication is used. For browser configuration instructions, access the [Websense Solution Center](#) and search for *How do I configure my web browser to support session-based authentication?*

Other technical limitations apply to the use of session-based authentication with certain web sites and applications. [Click here](#) for detailed information about these issues and how to resolve them.

See the [Websense blueSKY Security Gateway Release Notes](#) for information about this feature.

Authentication bypass for internal networks

You can bypass policy authentication settings based on the IP addresses in your internal networks, so that specific nodes in a network (for example, guest networks) are forced to authenticate using an alternative method, or are not authenticated at all.

Authentication bypass settings also control whether content analysis is performed based on internal IP addresses.

Configure bypass settings in the Authentication Bypass section of the **Web Security > Bypass Settings** page in the Websense blueSKY portal.

See the [Websense blueSKY Security Gateway Release Notes](#) for information about this feature.

Authentication decryption bypass for appliances



Important

This feature is available only with Websense Technical Support assistance.

You can now bypass SSL decryption for authentication purposes for IQ-Series appliance traffic that is subject to any type of authentication. This function allows you to choose whether to authenticate a user based on web category.

The appliance does not currently support authentication decryption bypass for custom categories.

Installation and upgrade

Topic 70118 | Release Notes | IQ-Series Appliance | Updated: 31-Oct-2014

Applies to:	Websense IQ-Series appliance v1.3, 1.3.1, 1.3.2
--------------------	---

Installation

Installation and set up for the Websense IQ-Series appliance are summarized on the Quick Start poster that was shipped with your appliance. [Click here](#) to view a copy of the quick start guide.

See the [Websense blueSKY Getting Started Guide](#) for information about system configuration.



Important

Use of Microsoft Internet Explorer 8 (or below) on a Windows XP machine is not supported.

If your network includes a firewall, you need to ensure that destination TCP ports are open for connection to the cloud service. By default, the appliance is configured to use standard destination ports 80 and 443 for these connections.



Note

Upgrade from a previous appliance version does not change port configuration settings. If you want to use destination ports 80 and 443, you should modify appliance settings manually after the upgrade process.

Alternatively, and depending on your corporate firewall policy, you can configure your appliance to use the following ports, which are used for non-appliance connections to the cloud service:

Port	Purpose
8002	Configuration and policy update information retrieval from Websense blueSKY. This port must be open for an IQ-Series appliance to retrieve periodic configuration setting and policy updates from the cloud service.
8081	Proxy service. This is where the Websense blueSKY cloud-based content analysis is provided.
80	Notification page components. The default notification pages refer to style sheets and images served from the Websense blueSKY platform. For these pages to appear correctly, this web site is accessed directly (i.e., not through Websense blueSKY).
443	Service administration. The Websense administration portal is similarly unproxied. Otherwise, it would be possible for you to accidentally block access and then be unable to rectify the situation.

You can switch between the standard and alternative ports at any time using the appliance command-line interface (CLI). See the [Websense blueSKY Getting Started Guide](#) for detailed instructions about switching port settings.

You should also open the outbound Network Time Protocol (NTP) port (UDP 123) to allow time/clock synchronization in the system.



Note

The transfer of new password and appliance registration information between the cloud portal and the appliance takes several minutes. You may experience a delay when logging in after a change is made to these settings.

Upgrade

Use the following steps to upgrade from a previous version of Websense blueSKY:

1. Click **Network Devices** in the cloud portal.
2. Select the appropriate appliance for the upgrade and click **Properties & Statistics**.
3. Click **Version History**.
4. Find the desired upgrade and click the **Download** icon in the Action column. This operation downloads the upgrade to the selected appliance.
Clicking the **View** icon in the Description column opens the Release Notes for that upgrade.
5. In the IQ-Series appliance **Configuration > Upgrade Management** page, find the upgrade in the table at the top of the screen. The upgrade status should be **Downloaded** (you may need to refresh the screen to see the change). Click the **Install** icon to install the upgrade.



Important

Upgrade status may display as “Failed” after a successful upgrade from version 1.2 to version 1.3. This incorrect error message may appear if you refresh the appliance user interface immediately after the upgrade operation.

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

If the problem persists after this time period, please contact Websense Technical Support.

Resolved and known issues

Topic 70119 | Release Notes | Websense IQ-Series Appliance | Updated: 31-Oct-2014

Applies to:	
	Websense IQ-Series appliance v1.3, 1.3.1, 1.3.2

Please contact Websense Technical Support for a list of known issues for this version of Websense blueSKY Security Gateway.

