Release Notes for Websense i-Series Appliances

Topic 70097 | Release Notes | i-Series Appliance | Updated: 13-Oct-2014

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

Contents

The Websense i-Series appliance is a component of Websense Cloud Web 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 i-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 Cloud Web Security Gateway analytics are applied and policy is enforced. Management of on-premises appliances is also performed in the cloud.

You can deploy the Websense i-Series appliance as a virtual appliance. For virtual appliance information, see the Websense Cloud Web Security Getting Started Guide.

View detailed product user information in the following Help systems:

- Websense i-Series Appliance Help
- Websense Cloud Security Help

Use these Release Notes to learn about version 1.3 product features, installation and upgrade tips, and resolved and known issues lists.

Version 1.3.1 release update

Topic 70098 | Release Notes | i-Series Appliance | Updated: 13-Oct-2014

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

This release of the Websense i-Series appliance addresses the following issues:

- **Bash vulnerabilities (Shellshock)**

  The critical Bash vulnerabilities that affect the Websense i-Series appliance 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 70099 | Release Notes | i-Series Appliance | Updated: 13-Oct-2014

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

This version of Websense Cloud Web 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 i-Series appliance:

- *Session-based authentication*
- *Authentication bypass for internal networks*
- *Authentication decryption bypass for appliances*

See the Websense Cloud Security Release Notes for detailed information about these cloud portal changes.

Session-based authentication

This release now supports session-based authentication for traffic that is routed through an i-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 cloud 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 Cloud Security Release Notes for more 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 cloud portal.

See the Websense Cloud Security Release Notes for more 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 i-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, deployment, and upgrade

Topic 70100 | Release Notes | i-Series Appliance | Updated: 13-Oct-2014

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

Installation

Installation and set up for the Websense i-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 Cloud Web Security 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 Cloud Security. This port must be open for an i-Series appliance to retrieve periodic configuration setting and policy updates from the cloud service.
8081	Proxy service. This is where the Websense Cloud Security cloud-based content analysis is provided.
80	Notification page components. The default notification pages refer to style sheets and images served from the Websense Cloud Security platform. For these pages to appear correctly, this web site is accessed directly (i.e., not through Websense Cloud Security).
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 Cloud Web Security 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.

Deployment

Additional considerations should be examined for some i-Series appliance deployments, including those that use:

- an i-Series virtual appliance
- endpoint devices or PAC-enabled clients that communicate directly with the cloud

Virtual appliance

The i-Series virtual appliance may be deployed with or without the network bypass capability. Download the appliance image (OVF format) from the MyWebsense Downloads page, and see the Websense Cloud Web Security Getting Started Guide for virtual appliance deployment instructions.

> **Note**
> If you want to deploy a virtual appliance with the network bypass capability, your hardware must support the ESXi DirectPath I/O function.

If you plan to deploy a virtual appliance, you should verify the following system requirements:

- VMware vSphere ESXi platform versions 5.1 or 5.5
- 6 CPU cores, 12 GB RAM (minimum)
- 128 GB hard disk drive
- Optional: Silicom network bypass card (Silicom PE2G2BPI80-SD-R) with 2 dedicated network interfaces (must be installed on ESXi in VMDirectPath mode)

  Some models of HP hardware do not support VMDirectPath mode.

Mixed-mode deployment issues

If your network includes an i-Series appliance along with endpoint devices or PAC-enabled clients that communicate with the cloud directly (for example, roaming users), you may encounter additional deployment issues. You should consider the following port information before you deploy:

- Use of the site's egress as a policy connection is not supported. As a result, endpoint or PAC-enabled clients are treated as roaming users regardless of whether they are connected within the network LAN.
- Endpoint device and PAC-enabled client traffic directly to the cloud service in a network that includes an i-Series appliance is supported on ports 8081 and 8082.
- Endpoint device traffic directly to the cloud service in a network that includes an i-Series appliance is supported on port 80, but traffic from a PAC-enabled client on port 80 is not supported.
- Applications that use HTTP (e.g., IM clients) may still try to use port 80 or 443 for outbound traffic. This traffic is intercepted and processed by the i-Series appliance, which may lead to inconsistencies. This potential problem should be checked on a per-site, per-application basis, and a resolution determined based on a customer's actual needs, for example:
  - Block the applications at the firewall level
  - Use explicit proxy mode for the applications
  - Use other ports for the applications

Upgrade

Use the following steps to upgrade from a previous version of Websense Cloud Security i-Series appliance:

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 i-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 70101 | Release Notes | Websense i-Series Appliance | Updated: 13-Oct-2014

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

A list of resolved and known issues for the Websense i-Series appliance is available in the Websense Technical Library. If you are not already logged on to MyWebsense, this link takes you to the log in screen.