Release Notes for Websense i-Series Appliances

Topic 70180 | Release Notes | i-Series Appliance | Updated: 01-Mar-2016

Applies to:	Websense i-Series appliance v1.6

Contents

- *Version 1.6 product features*
- *Installation, deployment, and upgrade*
- *Resolved and known issues*

The Websense® i-Series™ appliance is a component of Websense TRITON AP-WEB with the Cloud Web Module. This web protection solution 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.
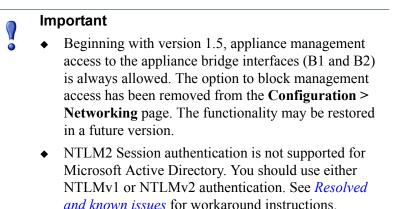
When analysis indicates that a web request requires further examination, the appliance transparently routes that traffic to the cloud, where Websense cloud service analytics are applied and policy is enforced. Management of on-premises appliances is also performed in the cloud.

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

View detailed product user information in the following Help systems:

- Websense i-Series Appliance Help
- Websense Cloud TRITON Manager Help

Use these Release Notes to learn about version 1.6.0 product features, installation and upgrade tips, and resolved and known issues.

> **Important**
>
> ◆ Beginning with version 1.5, appliance management access to the appliance bridge interfaces (B1 and B2) is always allowed. The option to block management access has been removed from the **Configuration > Networking** page. The functionality may be restored in a future version.
>
> ◆ NTLM2 Session authentication is not supported for Microsoft Active Directory. You should use either NTLMv1 or NTLMv2 authentication. See *Resolved and known issues* for workaround instructions.

Version 1.6 product features

Topic 70181 | Release Notes | i-Series Appliance | Updated: 01-Mar-2016

Applies to:	Websense i-Series appliance v1.6

This section of the Release Notes describes the new features that are included in version 1.6 of the Websense i-Series appliance:

◆ *Multiple policies for an appliance-managed network*
◆ *Traffic monitor*
◆ *Pre-installed category database*
◆ *Improved system infrastructure*

See the Websense TRITON AP-WEB (cloud) Release Notes for detailed information about all cloud portal changes.

Multiple policies for an appliance-managed network

In this version of the appliance, you can apply multiple policies to an individual appliance. Each policy applies to the traffic sent to the appliance from a specific internal network range. In previous versions, only a single policy could be applied to all the traffic sent to an appliance.

You define an internal network and assign a policy other than the default to that network in the cloud portal Network Devices page. See the topic titled Adding or editing an appliance in the Cloud TRITON Manager Help for details.

Traffic monitor

A traffic monitor is included in this version to display detailed information about web requests and protocol transactions. The monitor is accessed from the appliance command-line interface (CLI). You can indicate the traffic attributes you want to view in the monitor via CLI commands. Examples of attributes include:

◆ Source or destination IP address

◆ Date-time of the web request

◆ Policy name

◆ Protocol

◆ Web request URL

◆ Client browser

◆ Web category of the request

Click here for more details about configuring the traffic monitor.

Pre-installed category database

In previous versions, the i-Series appliance did not include the web category database out of the box. A full database download occurred after appliance registration, a process that could take a few hours. The appliance could not analyze any traffic until the long download process was complete.

The appliance now ships with a pre-installed web category database. After appliance registration, an update to this database is initiated. During the update, the appliance can analyze traffic using the pre-installed database. Note that because this database is out-of-date, traffic analysis may be more accurate after the full update is complete.

Improved system infrastructure

This version of the appliance includes several enhancements and fixes for system infrastructure that result in improved stability and security. In addition to an operating system upgrade, the release contains:

◆ Stability improvements for the authentication module and the Apache Traffic Server (ATS).

◆ Improved capacity to handle many policies along with a large volume of users

◆ Enhanced ability to set and view IP address to user mapping in the command-line interface (CLI)

◆ More complete report information for appliance traffic

◆ Cloud portal appliance date/time displayed using the current browser's time zone

- The following updates for SSL traffic flow support have also been made:
  - The intermediate certificate authority (CA) caching process is enhanced for increased reliability and security.
  - The method by which SSL traffic is encrypted is strengthened for increased security.
  - Certificate revocation list (CRL) operation is enhanced for reliability and improved maintenance.

Installation, deployment, and upgrade

Topic 70182 | Release Notes | i-Series Appliance | Updated: 01-Mar-2016

Applies to:	Websense i-Series appliance v1.6

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 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 that uses different default port settings does not automatically 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 the Websense cloud service. 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 Websense 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 service platform. For these pages to appear correctly, this web site is accessed directly (i.e., not through the Websense cloud service).
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 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

  See *Mixed-mode deployment issues* for information about handling traffic via these devices.

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 [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, 5.5, or 6.0
- 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. If the deployment requires the use of ports 80 and 443 for endpoint client traffic, please contact Websense Technical Support.
- When a Websense Endpoint requests a PAC file download, the cloud service can return a custom PAC file that first directs endpoint traffic to the appliance rather than redirecting it to the cloud service. Please contact Websense Technical Support for assistance to activate this feature.
- 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 inconsistent behavior. 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
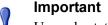- Use other ports for the applications

Upgrade

Use the following steps to upgrade from a previous version of the Websense 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. 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 70183 | Release Notes | Websense i-Series Appliance | Updated: 01-Mar-2016

Applies to:	Websense i-Series appliance v1.6

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.