# Release Notes for Websense i-Series Appliances

Topic 70045 | Release Notes | i-Series Appliance | Updated: 03-Dec-2013

| **Applies to:** | Websense i-Series appliance v1.1 |
|---|---|

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.

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 i-Series appliance features.

- *Product features*
- *Installation*
- *Known issues*

See the Websense Cloud Security Release Notes for updates on cloud portal changes. You must log on to the Cloud Security portal to view the Release Notes.

# Product features

Topic 70046 | Release Notes | i-Series Appliance | Updated: 03-Dec-2013

| **Applies to:** | Websense i-Series appliance v1.1 |
|---|---|

This section describes the major features available for the new Websense i-Series appliance.

## Websense i-Series appliance

The Websense i-Series appliance provides on-premises URL analysis and protocol detection, contributing to efficient Web request processing in your network. The Websense master Web category database is downloaded to and resides on the appliance, where it is updated periodically from the Websense database download server. The appliance is also a transparent proxy that can redirect traffic to Websense Cloud Security for analysis as needed. Updates to appliance configuration and policy settings occur regularly via communication with the Websense Cloud Security portal.

**Note**

Data sent between the Websense cloud portal and the on-premises appliance in either direction may take up to 15 minutes to take effect and be reflected in the cloud portal or appliance manager user interface.

The appliance includes a network bypass capability that allows Web traffic to flow when the appliance is in a hardware bypass state. The bypass capability may be needed to allow traffic flow when a network component is down for some reason. Communication with the Cloud Security portal is disrupted during any bypass interval.

You can also deploy the i-Series appliance as a virtual appliance. The virtual appliance may be deployed with or without the network bypass capability. Download the appliance image from the MyWebsense downloads page, and see the Cloud Security Getting Started Guide for system requirements and 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.

Use the appliance first-time configuration wizard to enter the important initial settings for appliance management. Establish the appliance host name, Web traffic and appliance management network interfaces, DNS servers, and network gateway. You must complete the wizard in order to manage the appliance.

You can monitor appliance system functions on the following appliance manager Status screens:

- General: See when the most recent Cloud Web Security Gateway update occurred, along with appliance licensing information and general system messages (e.g., updates on appliance operating status or upgrade availability).

- Resource Usage: View graphical representations of appliance resource usage, including CPU, memory, and disk space usage.
- Alerts: View appliance alerts from the past 24 hours.

Use the upgrade function to keep the appliance up-to-date for efficient operation. The **Configuration > Upgrade Management** screen lets you download and install the most recent appliance updates and view appliance upgrade history and upgrade Release Notes.

Other configuration screens allow you to view and modify the system configuration settings established in the first-time configuration wizard, including the appliance host name and interface and routing IP address designations.

The **Configuration > Registration** screen lets you manage your appliance registration with Websense Cloud Security. The **Administration > Account Management** page provides appliance password management capability.

See the appliance quick start poster for the steps needed to install and perform initial appliance configuration. See Websense i-Series Appliance Help for detailed information about all appliance features.

## Websense Cloud Web Security Gateway portal

Websense Cloud Web Security Gateway provides centralized management in the cloud for all the appliances in your network. You can add or remove an appliance from your system via the Network Devices screen. When you add an appliance in the portal, you also provide the following information:

- Appliance name, description, assigned Web policy, policy time zone, and cloud forwarding
- IP addresses for trusted Web traffic sources and destinations, HTTP/HTTPS port numbers, and IPv6 support handling options
- NTLM authentication domain and user revalidation interval
- Public certificate information

If the user is a technical support administrator, a Custom tab displays a table that contains the most recent 50 appliance configuration changes implemented by Technical Support. An administrator can add, view, or undo a configuration change in this tab.

The Network Devices screen also lets you obtain a registration key for the appliance and change the appliance password.

Status information about each appliance appears on the Network Devices screen. View at a glance whether an appliance is enabled, registered, and connected to the network. See appliance alerts for a user-defined time period and the name of the Web policy to which the appliance is assigned. The date/time of the most recent response from the appliance also appears.

A Properties & Statistics link takes you to a page with the following information:

- General appliance information, such as host name, and appliance version
- Appliance upgrade history and management, showing both installed upgrades and upgrades currently available for download to the appliance
- Charts illustrating appliance statistics, like resource usage and Web transaction rates

Centralized management in the portal includes the ability to configure how a policy handles protocols, or non-HTTP Web traffic. Websense provides a group of default protocols in a master database, to which you can add custom protocols (**Policy Management > Protocols**). In the Protocols tab for an individual policy (**Policy Management > Policies**), specify how Websense Cloud Web Security Gateway treats a protocol when detected and define individual user or user group exceptions that override policy action for a particular protocol.

Create custom categories to suit your individual needs, or import custom categories from a Websense Web Security on-premises solution if you have it (**Policy Management > Categories**).

**Note**

If you want to use transparent NTLM authentication, you must configure your end users’ browsers to support transparent NTLM authentication, either manually or via GPO or similar. See the Websense Cloud Security Getting Started Guide for details, in the topic titled *Enabling browsers for NTLM transparent authentication*.

See the Websense Cloud Security Getting Started Guide for information about configuring your Cloud Security network. See Websense Cloud Security Help for detailed information about these features.

See the Websense Cloud Security Release Notes for updates on cloud portal changes. You must log on to the Cloud Security portal to view the Release Notes.

## 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.
- The use of port 80 for endpoint device and PAC-enabled client traffic to the cloud service in a network with an i-Series appliance is not supported.

- Applications that use HTTP/S (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

# Installation

Topic 70047 | Release Notes | i-Series Appliance | Updated: 03-Dec-2013

| Applies to: | Websense i-Series appliance v1.1 |
|---|---|

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.

If your network includes a firewall, ensure that the following destination TCP ports are open:

| 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. |

It is also recommended that the outbound Network Time Protocol (NTP) port (UDP 123) be open as well 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.

# Known issues

Topic 70048 | Release Notes | Websense i-Series Appliance | Updated: 03-Dec-2013

| | |
|---|---|
| **Applies to:** | Websense i-Series appliance v1.1 |

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.