Websense i-Series Appliance Help

Help | i-Series Appliance | Version 1.2

The Websense® i-Series™ appliance provides on-premises URL analysis and application/protocol detection for Web request traffic. Real-time security capabilities on the i-Series appliance provide Web filtering with dozens of default URL categories.

When on-premises analysis indicates that a Web request requires further examination, the appliance transparently routes that traffic to the cloud, where Websense Cloud Security analytics are applied and policy is enforced. See Websense Cloud Web Security Help for information about the cloud portal.

A pass-through card allows traffic to flow through your network even if the appliance is not functioning properly or a network component is down.

A virtual i-Series appliance in OVF format is available on the MyWebsense Downloads page. The pass-through function is an add-on feature for the virtual appliance. Unless otherwise stated in the Help, virtual appliance functions are the same as the physical appliance.

Appliance help topics include:

Appliance quick start

Help | i-Series Appliance | Version 1.2

Before you begin the appliance quick start setup instructions, you should consider the following issues:

- If you plan to deploy a physical appliance, determine appliance rack location.
- If you plan to deploy a virtual appliance, verify your 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.

- Determine appliance IP addresses for network deployment.
- The database download initiated at the end of the setup may take a few hours, during which all traffic is permitted. A download progress message and status indicator displayed on the **Status > General** page disappear when the download is complete. This message appears only for this initial download.
- If your network includes a firewall, ensure that destination TCP ports 80, 443, 8002, and 8081 are open. See *Appliance network connection*, page 3, for details.
- It is also recommended that the outbound Network Time Protocol (NTP) port (UDP 123) be open to allow time/clock synchronization in the system.

Initial Websense Cloud Web Security settings

Perform the following steps in the Cloud Web Security portal:

1. Ensure that your Cloud Web Security account is established.
2. Log in to the cloud portal.
3. Click **Network Devices** in the Cloud Security console to display a list of your network appliances.
4. Click **Add** and enter new appliance information. See Websense Cloud Security Help for detailed information.

Important

It is recommended that you define certificates when you add an appliance, in order to avoid browser warnings regarding SSL termination for block, authentication, or quota/confirm operations.

Be sure to perform the following:

- Generate a CA certificate. Ensure that the certificate is not encrypted.
- Import this certificate to all relevant browsers.
- Upload this certificate to each appliance using the Certificates tab.

See the Getting Started Guide for detailed instructions.

You should also install a Websense Root Certificate to implement SSL decryption. See the Defining Web Policies topic in Websense Cloud Web Security Help.

Appliance setup and configuration

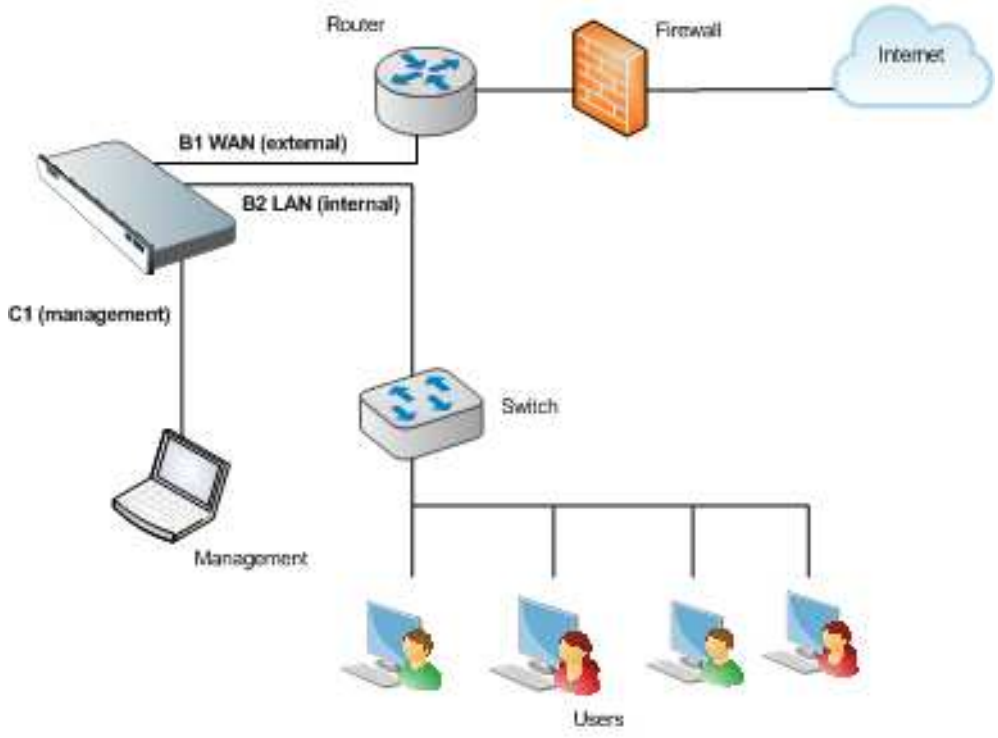
Perform the following steps to set up and configure a physical appliance:

1. Verify the contents of the accessory box that was shipped with the appliance. It should include power cable, an appliance bezel, and a quick start poster.
2. Rack the appliance and plug it in.
3. Power the appliance on and allow the boot sequence to complete.
4. Connect a computer with DHCP enabled (such as a laptop) to the appliance C1 interface. Wait a few moments, until the automatic network setup process is complete, to begin appliance configuration.
5. Log on to the appliance via a Web browser connection (https://169.254.0.2). Credentials are admin/admin.
6. Complete the appliance First-Time Configuration Wizard. See *First-time configuration wizard*, page 4, for wizard instructions.
7. Log off the appliance and disconnect the computer from the appliance.

See the Getting Started Guide for information regarding virtual appliance setup and configuration.

Appliance network connection

Connect the appliance to your network. The sample diagram shows a possible deployment:



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 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 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 Cloud Security platform. For these pages to appear correctly, this Web site is accessed directly (i.e., not through 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 should also open the outbound NTP port (UDP 123) to allow system time/clock synchronization.

Appliance registration

Perform the following steps to register the appliance with Cloud Security:

1. In the Websense Cloud Security console, click **Network Devices**.
2. Select the row that contains your new appliance and click **Register**.
3. Copy the registration key to the clipboard.

Appliance registration completion and password change

Perform the following steps to complete appliance registration:

1. Reconnect to the appliance using the management IP address (C1) or the default address (169.254.0.2) and log in.
2. Change the appliance password if you have not already done so.
3. Paste the Cloud Security registration key into the **Registration key** field.

At this point, the initial Web category database download starts. This download may take a few hours, during which time all Web traffic is permitted in your network.

A download progress message and status indicator displayed on the **Status > General** page disappear when the download is complete.

First-time configuration wizard

The Websense i-Series appliance First-Time Configuration Wizard walks you through some initial settings that are important for appliance operation. You must complete the wizard before you can manage the appliance. Cancelling the wizard before completing initial appliance configuration logs you out of the appliance, and any settings you may have entered up to that point are not saved.

Before you begin the wizard, you must perform the following tasks:

- Rack your appliance and plug it in (if you are deploying a physical appliance).
- If you are deploying a virtual appliance, download the OVF file and deploy your virtual appliance. See the Getting Started Guide for details.
- Power the appliance on.
- Connect a computer to it. Ensure the computer has DHCP enabled.
- Access the appliance manager via a Web browser.

See *Appliance quick start*, page 1, for details.

Click **Next** on the Welcome page to start the wizard.

Appliance host name

In the Host Name page, enter the appliance host name or fully qualified domain name (FQDN). The name may consist of 1 - 32 alphanumeric characters, dashes, and periods. It must begin with a letter and cannot end with a period.

Format for an appliance hostname is:

hostname

You can also use the format *hostnam.parentdomain*.

Format for the FQDN is:

hostname.parentdomain.com

Click **Next** to continue with the wizard.

Appliance network interfaces

The Network Interfaces page lets you configure your appliance interfaces for outbound traffic and appliance management. You can also designate your DNS servers on this page.

Web traffic and appliance management

Specify the appliance IP address and subnet mask in the Outbound Traffic section for the network bridge created by the B1 and B2 interfaces. These interfaces are used for

all outbound traffic. One interface (B1) handles traffic routed out of your network, and the other (B2) handles traffic to your internal network.

> **Note**
> Ensure you have configured valid routing between the bridge interface and any client generating traffic that is intercepted by the appliance (either explicitly for management purposes or transparently for authentication, quota, or confirm actions), taking the VLAN tag into account.
>
> See *VLAN tag*, page 8, for more information.

Provide the IP address and subnet mask for the C1 interface in the Appliance Management section. The C1 interface is used for appliance management functions. This interface can also be used when the B1/B2 bridge interface is in hardware bypass mode.

You can allow appliance management via the B1 and B2 bridge interfaces along with the C1 interface. Mark the **Allow appliance management access in addition to the C1 interface** check box to enable this capability. This is the default configuration.

> **Note**
> Although by default you may access the appliance manager via either the bridge or management interfaces, use of the management interface for this function is recommended.

If you are deployed on a virtual appliance that does not include the appliance bypass function, use of the C1 interface for appliance management is optional. If you do not define a C1 management interface, then you must use the B1/B2 bridge interface for management purposes. The **Use this interface for appliance management** check box is marked and not user accessible.

If you mark the **Use a dedicated appliance management IP address** check box in the Optional Appliance Management section, you can enter the IP address and subnet mask for the C1 interface. The **Allow appliance management access in addition to the C1 interface** check box is then accessible for marking or clearing.

DNS servers

You must define a DNS server by entering its IP address in the **DNS Servers** section **IP address** field and clicking **Add**. The IP address appears in the DNS Server IP Address list.

You may define up to 3 DNS servers, and you cannot define any 2 servers with the same IP address.

After you select an IP address in the DNS Server IP Address list, you can:

- Remove the address by clicking **Remove**.

- Move the address up or down in the list, to change the order in which the servers are used to process traffic. Use the up or down arrow to move a selected address, as appropriate.

Click **Next** to continue with the wizard.

Routing

The Routing page lets you define your default gateway, along with any static routes you may need. You can also specify a VLAN tag for management traffic, which the appliance uses to communicate with Websense cloud and database download services. This tag may also be used by clients that communicate with the appliance bridge interface.

> **Note**
> Ensure you have configured valid routing between any client generating traffic that is intercepted by the appliance and the bridge interface, taking into account the VLAN tag that you define on this page.

Default gateway

On the Routing page, specify the IP address of your default gateway for outbound traffic.

In many cases, you need only a gateway specification on this page. However, you can use the Routing Table to configure static routes. Configuring routes on the main bridge interface should not be necessary. For more information, see the Getting Started Guide.

Static routes

To add static routes, click **Routing Table**, and then **Add**. Provide the following route information in the Route Properties dialog box:

- Destination network
- Subnet mask for the destination network
- Gateway IP address
- Interface used. In the drop-down list, select either **Bridge (B1, B2)** or **Management (C1)**.

You may edit route properties by clicking the route destination network IP address link to open the Route Properties dialog box.

Remove a route from the table by marking the check box to the left of the desired route's row and clicking **Remove**.

VLAN tag

The appliance can be configured to analyze virtual LAN (VLAN) tagged and untagged traffic. All VLAN traffic is analyzed unless you define some of that traffic as trusted. You can bypass analysis for untagged traffic and for specific VLAN tags in the Websense Cloud Security portal. See the Getting Started Guide for configuration details.

The appliance supports the use of a single VLAN tag for management communication traffic from the appliance to the cloud and database download services. This tag is also used by any client that communicates with the appliance bridge interface (B1 and B2) either explicitly for management purposes or transparently for authentication, quota, or confirm actions.

Activate VLAN tag support by marking the **Use the following VLAN tag** check box. Enter the desired tag in the entry field using a number from 0 to 4094.

> **Note**
> If you change the VLAN tag while your client is connected to the appliance management interface, you may lose connectivity with the appliance. Ensure that your client routing includes the new VLAN configuration to recover the connection.

Click **Next** to continue with the wizard.

Finish

The final page of the wizard summarizes the entries and selections you have made. If you want to change any setting after your review, click **Back** to access the desired wizard page and edit your settings.

If you are satisfied with your settings, click **Finish**.

At this point, you are logged off the appliance. You must log back in for your configuration settings to take effect.

When you log back in, you are prompted to change your initial password (if you have not already done so) and register the appliance with Websense Cloud Security. See *Appliance registration*, page 9, for information.

> **Note**
> If you are unable to access the appliance, you can connect to the appliance manager interface at any time via https://169.254.0.2.

Appliance registration

Help | i-Series Appliance | Version 1.2

In order to manage your appliance, you must change the initial password and register the appliance with Websense Cloud Security.

When you log back in to the appliance after completing the First-Time Configuration Wizard, the initial screen lets you change the initial password, if you have not already done so, in the Administrator Credentials box. If you changed the password before completing the wizard, the Administrator Credentials box does not appear on this page when you log back in.

This initial page also lets you enter your Cloud Security registration key. You should already have added this appliance to the Network Devices list in the Websense Cloud Security portal. See *Appliance quick start*, page 1, for information.

To register your appliance:

1. Log on to the cloud portal and click **Network Devices**.
2. Select the row that contains this appliance.
3. Click **Register** at the bottom of the page to open the Register Appliance box.
4. Copy the displayed registration key and click **Close**.
5. Return to the appliance manager and paste the key into the **Registration key** field.
6. Click **OK**.

The appliance **Status > General** page appears and the initial Web URL category database download to the appliance starts. This first download activity may take a few hours to finish.

A download progress message and status indicator appear on the **Status > General** page. The message and indicator disappear when the initial download is complete.

During the initial download, all Web traffic is permitted in your network.

General configuration

Help | i-Series Appliance | Version 1.2

The appliance **Status > General** page displays the current status of Websense Cloud Security updates and license information. It can also contain a collection of information or warning messages regarding appliance configuration settings and status.

Websense Cloud Security updates

The i-Series appliance periodically retrieves configuration and policy updates from Websense Cloud Security. This section of the **Status > General** page displays the date

and time of the most recent configuration and policy update from Cloud Security, along with the most recent connection date/time. Updates occur approximately every 2 minutes. If more than 15 minutes elapse between updates, the date/time display appears in red, and you should investigate why updates have not been retrieved.

The updates section also includes a link that, when clicked, initiates an immediate update from Cloud Security. This link is helpful when the update interval is significantly longer than 5 minutes (for example, after 15 minutes, when the date/time display turns red).

Appliance license information

The License section contains information about the current appliance license, including the following details:

- Services provided by the license
- Type of license (e.g., evaluation, purchase)
- Number of users allowed
- Period during which the appliance license is valid

Configuration and status information

The **Status > General** page may contain several information or warning messages, depending on the current status of the appliance. The following messages may be displayed:

- **Web category database download is in progress.** This message appears only during the initial Web category database download operation started after a successful appliance setup and configuration. The appliance allows all Web traffic to proceed while the download is in progress. A progress indicator displays the status of the download process. The message disappears when the download is complete.
- **Change password.** This message appears if you have not changed the initial appliance password. Clicking the **Change password** link takes you to the **Administration > Account Management** page, where you can change the appliance password.

  If you have changed the initial password, this message does not appear in the **Status > General** page.
- **Register the appliance.** This message appears if you have not registered the appliance with Websense Cloud Security. Clicking the **Register the appliance** link takes you to the **Configuration > Registration** page, where you can enter the registration key obtained from the Cloud Security portal. See *Appliance registration*, page 9, for details.

  If you have registered the appliance with Cloud Security, this message does not appear in the **Status > General** page.
- **The appliance is in bypass mode.** This message indicates that the appliance is in a hardware bypass situation and is not currently monitoring network traffic. All

network traffic continues to flow, even if the appliance is powered down. Communication with Cloud Security is compromised while the appliance is in bypass mode. Clicking the link takes you to the **Configuration > System** page, where you can change appliance mode to active.

If the appliance is in active mode, this message does not appear in the **Status > General** page.

- **The appliance has been disabled via a Websense cloud portal operation.** This message indicates that the appliance is disabled in the Cloud Security portal. All Web traffic flows through the appliance, and communication with Cloud Security continues. However, no Web policy is applied to the traffic.

  To enable your appliance, log on to the cloud portal and locate the appliance on the Network Devices page. Click the appliance name in the list, mark the **Enabled** check box in the General tab, and click **OK**.

  If the appliance is enabled, this message does not appear in the **Status > General** page.

- A series of appliance upgrade-related messages may appear at various times.
  - **Appliance update is available. Please upgrade this appliance.** Displayed with an information icon, this message indicates that an appliance upgrade has been released. Upgrade installation is recommended. Clicking the message link takes you to the **Configuration > Upgrade Management** screen, where you can initiate upgrade installation.
  - **Appliance update is available. Please upgrade this appliance within *[x]* days.** (where ***x*** is a value from 7 to 14) Displayed with a warning icon, this message indicates that your product version must be upgraded within 7 to 14 days, or you will lose your **Websense Cloud Security** connection. Clicking the message link takes you to the **Configuration > Upgrade Management** screen, where you can initiate upgrade installation.
  - **Appliance update is available. Please upgrade this appliance within *[x]* days.** (where x is a value less than or equal to 7) Displayed with an error icon, this message indicates that your product version must be upgraded within 7 days, or you will lose your **Websense Cloud Security** connection. Clicking the message link takes you to the **Configuration > Upgrade Management** screen, where you can initiate upgrade installation.
  - **This appliance was not upgraded by the specified date. Connection to Websense Cloud Security has been lost.** Displayed with an error icon, this message indicates that your appliance was not upgraded within the required amount of time. Traffic still flows through the appliance, but it is no longer connected to Websense Cloud Security and no traffic analysis occurs. Category database downloads are discontinued. You must contact Websense Technical Support for information regarding the restoration of your service.

- ***x* Alerts found (last 24 hours).** This message indicates how many alerts the appliance has generated in the past 24 hours. Clicking the link takes you to the **Status > Alerts** page, where you can view a list of alerts, their severity, and the date/time each was generated. An Alert Details box displays more information about why a selected alert occurred and how you might resolve a warning or error situation.

Resource usage

Help | i-Series Appliance | Version 1.2

The appliance **Status > Resource Usage** page displays 3 charts that detail the current status of appliance resources. The charts show statistics for the point in time at which they are opened. To see updated resource usage information, you must refresh the screen.

The charts show the usage levels for the following resources:

- CPU capacity
- Memory
- Disk space

These graphs can be useful for troubleshooting some appliance performance issues.

For more graphical information showing transaction rates and bandwidth usage, view appliance statistics in the Cloud Security portal. On the Network Devices page, click the **Properties & Statistics** link and open the **Statistics** tab. Select a chart from the drop-down list.

Alerts and diagnostics

Help | i-Series Appliance | Version 1.2

The **Status > Alerts and Diagnostics** page displays 2 tabs: Alerts and Diagnostics. The Alerts tab displays appliance alert events from the previous 24 hours, along with the date/time of alert occurrence. The alerts are sorted by date, with the most recent alerts appearing at the top of the list. The Diagnostics tab lets you execute a series of tests to determine system connectivity status and health.

Alerts

An alert is characterized as having 1 of 4 severity levels:

- Info: An informational message that does not require a user response
- Warning: A message that provides advance notice of an impending error situation that may require a user response
- Error: A message that describes an error situation that requires user attention
- Critical error: A message that describes an error situation that requires immediate user attention

Select an individual alert in the list to display detailed information that describes the issue and may offer possible resolutions to that issue.

The Cloud Security portal also contains a history of appliance alert events in the Network Devices page. Up to 7 days of alerts may be viewed.

Appliance upgrade alerts displayed on the **Status > Alerts and Diagnostics** page are also sent via email from the Cloud Security portal.

Diagnostics

The Diagnostics tab provides the capability to run a series of system tests to determine the current state of Websense Cloud Security. The first time you open the Diagnostics tab, a table shows a list of the tests to run. The tests include, for example, a status check of the network interfaces, the default gateway, your DNS servers, or the cloud connection.

Click **Run Diagnostics** to start the tests. The Results column displays test status (In progress) and results (Passed, Failed, or Could not complete). For tests that do not complete or fail, the Details column displays more information, including suggestions for resolving the issue that caused the failure.

Each time you open the Diagnostics tab thereafter, the most recent test results appear, along with the date/time of those tests.

System information

Help | i-Series Appliance | Version 1.2

The **Configuration > System** page displays current information about the appliance, including appliance version, platform, the appliance date/time determined by Cloud Security, and how long the appliance has been running since the most recent appliance restart.

You can also select 1 of the following operating modes for the appliance:

- Active
- Bypass

Note

The bypass mode applies to a virtual appliance deployment only when a network bypass card is present.

An appliance in active mode is monitoring network traffic, provided the appliance is registered and enabled in the Cloud Security portal (**Network Devices > Add/Edit Appliance**). If the appliance is not enabled in Cloud Security, traffic continues to flow through the appliance and is monitored, but no Web policy is applied.

When an appliance is in bypass mode, Web traffic is not monitored although it continues to flow. In a hardware bypass situation, all traffic is permitted, but communication with Cloud Security is compromised.

The button to toggle appliance operating mode is labelled **Activate** or **Bypass**, depending on the current appliance mode. Click **Activate** to allow an appliance in bypass mode to begin monitoring network traffic. After appliance activation, click **Bypass** to place the appliance in bypass mode if desired.

> **Note**
> When you switch from 1 appliance operating mode to the other, link autonegotiation causes a short outage (less than 10 seconds) on the bridge interfaces.

You may perform the following appliance operations on the System page:

- Reboot
- Power off

Click **Reboot** to restart the appliance, and click **Power off** to turn off appliance power.

The appliance host name or FQDN that you entered in the First-Time Configuration Wizard appears in the **Host name or FQDN** field. See *Appliance host name*, page 5, for details. You can edit the host name on this page.

Network interfaces and routing

Help | i-Series Appliance | Version 1.2

The **Configuration > Interfaces and Routing** page contains 2 tabs: Interfaces and Routing. The first time you open this page, the Interfaces tab displays the network interface settings and DNS server designations that you configured in the First-Time Configuration Wizard. Likewise, the Routing tab displays the default gateway, static routes, and the VLAN tag you defined in the wizard's Routing page.

You may edit network interface and routing settings on this page. See *Appliance network interfaces*, page 5, for information about configuring network interfaces and DNS servers. See *Routing*, page 7, for information about setting the default gateway, defining traffic routes, and specifying a VLAN tag.

Registration

Help | i-Series Appliance | Version 1.2

Register your appliance with Websense Cloud Security on the appliance **Configuration > Registration** page.

If you have not registered your appliance, you should obtain the key from the Cloud Security portal Network Devices page and enter it here. Click **OK** to register the appliance. See *Appliance registration*, page 9, for instructions on obtaining an appliance registration key from Cloud Security.

If you have not changed the appliance initial password, this page is not available for registration key entry. You must change the initial password (**Administration > Account Management**), then obtain your registration key from Cloud Security and enter it in the Registration page.

Appliance upgrade management

Help | i-Series Appliance | Version 1.2

Use the **Configuration > Upgrade Management** page to keep the appliance up-to-date with the latest releases. You can check for, download, and install product upgrades from this page. The current appliance version and date of installation appear at the top of the page.

The appliance checks for available upgrades on a daily basis. You receive alerts regarding upgrade availability on the **Status > General** page. See *Configuration and status information*, page 10, for information about these messages.

When a new upgrade is available, its version number, availability date, description, and status are displayed in the upper table with a status of **Available**. Clicking the icon in the Description column opens the Release Notes for that version.

The Action column contains icons that, when clicked, initiate the next appropriate action for an upgrade. For example, an available upgrade can be downloaded. An upgrade that has already been downloaded (and has a status of Downloaded) can then be installed. Note that after an upgrade is downloaded or installed, you must refresh the screen in order to change upgrade status.

Depending on your network bandwidth, download operations can take some time. You should note that upgrade installations initiate an appliance bypass condition and cause the appliance to reboot.

The Upgrade History table provides a record of upgrade releases that have been applied to the appliance, including version number, upgrade date, and status (e.g., successful or unsuccessful download and installation). The Action column contains icons that open the Release Notes for an installed upgrade or a download/installation log file.

Account management

Help | i-Series Appliance | Version 1.2

Change the appliance password on the **Administration > Account Management** page. The password must be 8 - 30 alphanumeric characters.

Enter the current password, then enter and confirm the new password. Click **OK**.

A password strength indicator rates your password on the basis of how many uppercase and lowercase characters are used, along with numbers and special characters. Use of at least 2 elements from each area contributes to password strength.

If you have not already changed the initial appliance password, you should change it on this page.

If you forget your appliance password and cannot log in, use the following steps to change the password:

1. Connect to the Websense cloud portal.
2. Click **Network Devices** and select the appropriate row in the Appliances list for your appliance.
3. Click **Change Password** at the bottom of the page, then enter and confirm a new password.

   You should wait a few minutes before you use the new password, to allow it to be updated on the appliance.