Getting Started Guide

Websense® blueSKY™ Security Gateway

2015 Release 3 and later

10900 Stonelake Blvd, 3rd Floor, Austin, TX 78759, USA

Published 2015
Printed in the United States of America and Ireland.

Trademarks

This product includes the following:

Sha512Crypt.java Java Port

Contents

1 Introduction

Welcome to the *Websense® blueSKY Security Gateway Getting Started Guide*. Websense blueSKY provides on-premises URL analysis and application/protocol detection for Web traffic through an IQ-Series™ appliance, along with centralized policy management and reporting capabilities in the cloud. When policy indicates that a Web request requires more than on-premises analysis, that traffic is transparently routed to the cloud, where Cloud Security analytics are applied and policy is enforced.

Websense blueSKY is simple to use and works "out of the box" with a default policy. To make full use of its features, however, you should configure your policy. This guide outlines the tasks that you must complete to get Websense blueSKY filtering your Web traffic.

Further Information

Detailed configuration advice for Websense blueSKY is available in the Websense blueSKY Security Gateway Help.

The Knowledge Base also contains technical information that is not included in this guide, such as common configuration questions and known issues with workarounds. The Knowledge Base also allows you to search for answers to a question you may have. Enter a search phrase into the entry field and search all categories to see all the articles in a given category. A list of related articles appears.

You should check these resources whenever you experience a problem or have a support question.

Getting Started

The following steps must be completed before you can use Websense blueSKY. **It is important that you follow these in order**:

1. Request a Websense blueSKY account. This account enables you to log on to the cloud portal and set up your service. See *Requesting a Websense blueSKY Account*.
2. Prepare for the deployment process, including the appliance rack location and configuring your firewall. See *Issues to consider before you begin*.
3. Log on to the Websense blueSKY portal, perform your first directory synchronization, and add your new appliance. See *Initial portal settings*.
4. Set up your appliance, and connect it to the network. See *Appliance setup and configuration*.
5. Register the appliance with Websense blueSKY. See *Registering the appliance*.
6. Decide how your end users should be authenticated, and configure your end users' browsers, if required, to enable transparent authentication. See *Setting Up End-User Authentication*.
7. Tailor your Websense blueSKY policy to meet the needs of your organization. See *Next Steps*.

Technical Support

If you have any questions during the set up phase, please contact your Websense reseller or Websense support. Technical information about Websense products is available online 24 hours a day, including:

- latest release information
- searchable Websense Knowledge Base
- show-me tutorials
- product documents
- tips
- in-depth technical papers

Access support on the Web site at:

http://www.websense.com/content/support.aspx

If you create a MyWebsense account, you are prompted to enter all Websense subscription keys. This helps to ensure ready access to information, alerts, and help relevant to your Websense products and versions.

The best practice is to create your MyWebsense account when you first set up your Websense blueSKY account, so that access is readily available whenever you need support or updates.

For additional questions, fill out the online support form at:

http://www.websense.com/content/contactSupport.aspx

2 Requesting a Websense blueSKY Account

If you are reading this guide, it is likely that you have already purchased Websense blueSKY Security Gateway or enrolled for a trial, and have a MyWebsense account. If not, see below for details of how to request one.

Existing Cloud Security customers

If you are an existing Websense Cloud Email Security customer or are performing a Cloud Email Security trial, you can request that Websense blueSKY be added to your account by contacting Websense Sales (contact details at the front of this document) or your Websense reseller. Websense Support notifies you by email when the services are added.

Alternatively you can request a trial online as described in *Requesting a trial*.

New customers

If you are new to Websense cloud-based services, you can request a trial online. For more information, see *Requesting a trial*.

Requesting a trial

Getting Started Guide | Websense blueSKY Security Gateway

1. Go to www.websense.com/bluesky and click **Request free trial**.

2. If you already have a MyWebsense account, log in on the page that appears. If you do not have a MyWebsense account, click **Register** and follow the steps to enter your details, then return to the product page and click **Request free trial** again.
3. Read the terms and conditions by clicking on the link, then check the box confirming you have read them and click **Confirm**.

   Shortly after you click **Confirm**, you receive an email message containing the links to the following:

   - the cloud portal
   - this guide
   - support options

   If you are new to Websense cloud-based products, the message also includes your portal username and a temporary password. You will be asked to change the password the first time you log on.

   If you are already a Websense cloud customer, Websense blueSKY Security Gateway is added to your account. Use your existing credentials to log on to the portal.

If you prefer to talk to a representative immediately, inside the U.S., call 1-888-546-1929. Outside the U.S., please visit http://www.websense.com/content/find-a-partner.aspx to locate a reseller.

Logging on to the Websense blueSKY portal

Getting Started Guide | Websense blueSKY Security Gateway

When you receive logon information in your confirmation email, log on to the Websense blueSKY portal by clicking the link that is provided or visiting https://bluesky.websense.net/portal.

> **Note**
> You must have port 443 open on your firewall to access the Websense blueSKY portal.

Enter your user name and password into the fields provided. If you are a new customer, you will be asked to change your password and set a password reminder question. You must also accept the terms of your license agreement to proceed.

You can now configure your Websense blueSKY account. See *Initial portal settings* for the configuration you must perform as part of the deployment process.

A default policy has been created for you: click **Web Security > Policy Management > Policies** to access it. This reflects the most commonly chosen policy options. Note that your IQ-Series appliance can be assigned to only one Web policy, so it is recommended that you edit this policy to meet your requirements. For more information, see *Next Steps*.

You can change your account configuration at any time. Refer to the Websense blueSKY Help for full instructions on how to configure your account. Click **Help** in the top right of the portal to access this guide.

3 Deploying Websense blueSKY

Once you have a Websense blueSKY account and have received your appliance, you can deploy Websense blueSKY Security Gateway by completing the following tasks:

1. *Issues to consider before you begin*
2. *Initial portal settings*
3. *Appliance setup and configuration*
4. *Connecting the appliance to your network*
5. *Registering the appliance*

The Quick Start poster, which is packaged in the appliance shipping box, outlines these tasks and includes a section for writing down reference information during deployment.

Issues to consider before you begin

Consider the following before you begin the deployment:

- Determine appliance rack location.
- Determine appliance IP addresses for network deployment. You will require 2 addresses and it is recommended that you configure 3.
- Determine your directory synchronization policy.
- If you wish to use transparent NTLM authentication for your users, decide whether to connect your appliance to a local Active Directory (see *Configuring Active Directory authentication*, page 19).

  If you plan to use Active Directory authentication, ensure that your appliance hostname complies with Active Directory hostname requirements (see *First-Time Configuration Wizard*, page 14).

Alternatively you can enter the domain that forms part of your users' NTLM identity when adding your appliance in the cloud service portal.

> **Note**
> To use your Active Directory for authentication, the appliance must be able to access the directory's IP address and port(s). You may need to edit an internal firewall setting or LAN routing rules.

- It is recommended that you provide a certificate when you add an appliance in the cloud portal, in order to avoid browser warnings regarding SSL termination for block, authentication, or quota/confirm operations. See *Generating a certificate*.

  To use the cloud service SSL decryption feature, you should also install the Websense root certificate on each client machine. See the section "Enabling SSL decryption" in the Websense blueSKY Help.
- The database download initiated at the end of the setup may take a few hours. This is a one-time operation, and traffic flows normally through the appliance during this time. A download progress message displayed on the **Status** > **General** page disappears when the download is complete.
- Browsing via the appliance has been tested with most commercially available web browsers. However, note that using a Windows XP machine with Internet Explorer 8 or below is not recommended, as HTTPS connections are not supported on appliances for this platform and browser.

Initial portal settings

Getting Started Guide | Websense blueSKY Security Gateway

You should have received your Websense blueSKY Security Gateway confirmation email, including a portal user name and temporary password if you are a new Websense cloud services customer, as described in *Logging on to the Cloud TRITON Manager*. The initial portal setup involves the following tasks:

1. *Run directory synchronization*
2. *Add new appliance information*.

Run directory synchronization

Getting Started Guide | Websense blueSKY Security Gateway

It is recommended that you use directory synchronization to import your users and groups information from your LDAP directory (for example, Active Directory) into the Websense blueSKY portal. This is the quickest and easiest way to import end

users' email addresses, and also NTLM details if you are planning to use NTLM identification.

> **Note**
> For alternatives to directory synchronization, see *Enabling browsers for NTLM transparent authentication*.

Although Websense blueSKY is a cloud-based service, it synchronizes with LDAP directories via a client-resident application called the Directory Synchronization Client. Changes made to a directory, such as deleting a former employee or adding a new one, are picked up by the service on the next scheduled update. If you have more than one LDAP directory, the client can merge them together before synchronizing the data with the service.

To set up and run directory synchronization:

1. Log on to the Websense blueSKY portal from the machine you want to use for directory synchronization.
2. Go to **Account Settings > Directory Synchronization**.
3. Download and install the appropriate version of the Directory Synchronization Client.
4. In the portal, go to **Account Settings > Contacts** and set up an administrator contact with Directory Synchronization permissions. The logon credentials you define will be used by the Directory Synchronization Client to log onto the portal.
5. Configure the Directory Synchronization Client as described in the *Directory Synchronization Client Administrator's Guide*, including the logon credentials you created in the previous step.

> **Note**
> If your LDAP data does not include users' email addresses, you can change the default attribute for the primary mail value in the Directory Synchronization Client as follows:
>
> - When creating or modifying the Users part of your configuration profile, go to the **Data source > LDAP** search page in the wizard. Click **Advanced** to display the Search attributes page.
> - In the Primary Mail field, replace %mail% with another attribute.
>
>   For example, you could use %userPrincipalName% if configured, or create a 'fake' email address using the sAMAccountName such as %sAMAccountName%@mydomain.com.

6. Once you are ready to synchronize data with the portal, go back to **Account Settings > Directory Synchronization**.

a. Click **Edit**.

b. Click **Enable directory synchronization**.

c. For **User policy assignment**, select Fixed.

d. For **Email new users**, define whether synchronized users should receive a notification email from Websense blueSKY.

e. Click **Submit** when done.

7. Run the synchronization, and check the results both in the client and on the portal:
   - In the client, click on the **Groups** and **Users** tabs to view the results.
   - On the portal, go to **Account Settings > Directory Synchronization**. The Recent Synchronizations section shows your recent synchronization history; click the timestamp in the date column to view details about a specific synchronization.

Add new appliance information

Getting Started Guide | Websense blueSKY Security Gateway

To add your new appliance information in the Websense blueSKY portal:

1. Click **Network Devices**.
2. On the Appliances tab, click **Add**.

> **Note**
> 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. See *Generating a certificate*.

3. In the General tab:
   a. Enter a unique appliance name (1 - 512 alphanumeric characters).
   b. Enter a brief description (maximum length of 1024 characters).
   c. Ensure the appliance is enabled by marking the **Enabled** check box (default setting). A disabled appliance can communicate with the cloud, but does not process web traffic and allows everything through.
   d. Specify the Web policy and associated time zone used to filter traffic from this appliance. The time zone should be that of the appliance's physical location.
   e. **Enable cloud forwarding** is checked by default. This means that web traffic is redirected to the nearest cloud service cluster for additional analysis. Uncheck this option if you do not want all traffic to be forwarded to the cloud. All traffic will be analyzed through the appliance, but without any cloud analytics.
4. In the Networking tab:
   a. Add IP addresses or address ranges whose traffic should not be analyzed in the Trusted Network Sources box. Click **Add** and enter either:

- IP or network address and subnet mask
- IP address range

Enter a suitable **Description** for the trusted network.

Select the traffic direction for the specified addresses as either **Source** or **Destination**.

Click **OK**. You can delete a trusted network entry by marking the check box next to it and clicking **Remove**.

> **Note**
> For the initial appliance deployment, we recommend that you configure all of your IP address ranges as trusted network sources, meaning that the appliance ignores all traffic. You can then test your deployment with a small number of clients before opening it up to all IP addresses and ignoring only those addresses whose traffic you do not want to be analyzed - for example, servers that receive Microsoft and antivirus updates.

b. For a network architecture that includes virtual LANs (VLANs), in the VLAN Tag Support section check **Support VLAN tags** if you want the appliance to analyze VLAN-tagged and untagged traffic. All VLAN traffic will be analyzed unless you define some of that traffic as trusted. You can bypass analysis for specific VLAN tags by entering trusted tag numbers in the **VLAN tag** field, and bypass analysis for untagged traffic by checking the **Trust untagged traffic** box.

   The appliance supports the use of a single VLAN tag to identify management communication traffic from the appliance to the cloud and database download services. You can configure this tag on the Routing page of the *First-Time Configuration Wizard*.

   > **Note**
   > The VLAN tag entered on the appliance Routing page is also used by any client that communicates with the appliance bridge interface, either explicitly for management purposes or transparently, for example for authentication, quota, or confirm actions when filtering. Ensure you have configured valid routing between the bridge interface and any client generating traffic that is intercepted by the appliance, taking the VLAN tag into account.

c. In the Ports section, enter comma-separated port numbers for HTTP and HTTPS channels.

d. Specify how the cloud service handles requests for IPv6 destinations (allow or block). Traffic to IPv6 destinations that is allowed (default setting) is not filtered or logged.

5. In the Authentication tab:
   a. If you wish to use transparent NTLM authentication and your appliance will not be connected to a local Active Directory, enter the domain that forms part of your users' NTLM identity. The NTLM domain is the first part of the domain\username with which users log on to their Windows PC; for example, MYDOMAIN\jsmith.

      Important
      You must configure your end users' browsers to support transparent NTLM authentication, either manually or via GPO or similar. See *Enabling browsers for NTLM transparent authentication*, page 80.

      If you are connecting your appliance to a local Active Directory for NTLM authentication, this field is not required as the appliance retrieves this information automatically from the local Active Directory.
   b. Select a time period after which a user's login and password must be revalidated from the **Session timeout** drop-down list. The default is 1 day.
   c. If you have users on a thin-client environment, define network addresses and IP address ranges that should use session-based authentication. In this environment, the mapping of end user to source IP address is no longer 1-to-1. To overcome this issue and authenticate end users correctly, session-based authentication takes place at configurable intervals by using cookies injected into the web traffic that force the web client to authenticate.

      Once a cookie is injected, it is analyzed by the appliance and serves as a replacement for the user-to-source IP address mapping to associate a specific transaction to a specific user. This authentication is then valid for the length of time defined in the **Session timeout** drop-down list.

      Note
      When session-based authentication is enabled, the **Allow end users to bypass all certificate errors** option on the portal Bypass Settings page is not currently supported.

6. In the Certificates tab:
   a. Specify the certificates used for this appliance:
      - Browse to the public certificate file. Open the file to enter its name in the **Public certificate** field.
      - Browse to the private key file. Open the file to enter its name in the **Private key** field.
      - If you have chained certificates, mark the **Add chained certificate** check box and browse to the intermediate certificate. Open the file to enter its name in the **Add chained certificate** field.

   For information on generating your own certificate for the appliance, see *Generating a certificate* below.

If you want to specify your certificates later, mark the **I want to define certificates later** option.

7. Click **OK**.

The appliance details are displayed on the Network Devices page. The appliance is also added as the proxied connection on the **Connections** tab of the policy that you specified, ensuring your policy is applied to all requests originating from the appliance.

Generating a certificate

We strongly recommend that each appliance has a valid X.509 identity certificate with an unencrypted key. This avoids browser warnings regarding SSL termination block, authentication, or quota/confirm operations.

The certificate can be generated using a variety of tools. Below is a simple procedure using OpenSSL to generate a private key and CA that can be used for your appliance.

This section assumes that you are familiar with OpenSSL and have a working OpenSSL installation.

The OpenSSL statement

```
openssl genrsa -passout pass:1234 -des3 -out
CA_key_password.pem 2048
```

creates a 2048-bit RSA private key with a password of 1234. You must supply a password, as OpenSSL does not allow the creation of a private key without one. You can then strip the password from the key as follows:

```
openssl rsa -in CA_key_password.pem -passin pass:1234 -out
CA_key.pem
```

This also renames the private key file from CA_key_password.pem to CA_key.pem.

Finally, use the following statement to create the CA:

```
openssl req -x509 -days 11000 -new -sha1 -key CA_key.pem -
out CA_cert.pem
```

Note that this command prompts you to input information about different parameters, such as country, state, locality, or your organization’s name.

Once you have created the private key (CA_key.pem) and public certificate (CA_cert.pem), import the certificate to all relevant browsers, and upload the certificate to each appliance using the Certificates tab.

Appliance setup and configuration

Perform the steps below to set up and configure your appliance. These steps are also described, with diagrams, on the Quick Start poster.

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*.
7. Log off the appliance and disconnect the computer from the appliance.

First-Time Configuration Wizard

Getting Started Guide | Websense blueSKY Security Gateway

The 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.

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

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

   The format for an appliance host name is *hostname*. You can also use the format *hostname.parentdomain.*

   The format for the FQDN is *hostname.parentdomain.com.*

   If you plan to use Active Directory authentication, the following hostname requirements are enforced:

   - Total length of 2 - 128 alphanumeric characters (including hostname and parent domain name elements; format is *hostname.parentdomain*)
   - May include dashes, underscores, and periods
   - Must begin with an alphanumeric character
   - Cannot end with a dash, underscore, or period
   - Hostname element length should be between 2 and 15 characters
   - Cannot match any of the following reserved words:

ANONYMOUS	BATCH	BUILTIN
DIALUP	INTERACTIVE	INTERNET
LOCAL	NETWORK	NULL
PROXY	RESTRICTED	SELF

SERVER	SERVICE	SYSTEM
USERS	WORLD	

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

2. On the Network Interfaces page:

   a. In the Outbound Traffic section, specify the appliance IP address and subnet mask 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.

   b. Provide the IP address and subnet mask for the C1 interface in the Appliance Management section. This 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 you may access the appliance manager via either the bridge or management interfaces, use of the management interface for this function is recommended.

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

      You can define up to 3 DNS servers. You cannot define more than one server with the same IP address.

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

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

   Note

   In many cases, you need only a gateway specification on this page. However, there may be cases where explicit or static routing is required. For more information on these scenarios, please see the knowledge article "Configuring routing for i-Series and IQ-Series appliances".

   If you need to define routing over the bridge interface, please contact Websense Technical Support in the first instance. You can define routing rules over the management interface as follows:

   Click **Routing Table**.

   Click **Add** and then 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)**.

   The appliance supports the use of a single VLAN tag to identify 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, either explicitly for management purposes or transparently, for example for authentication, or for quota or confirm actions when filtering.

   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.

   Mark the **Use the following VLAN tag** check box, then enter the tag in the entry field using a number from 0 to 4094.

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

4. 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**.

You must log off the appliance and log back on for your configuration settings to take effect.

When you log back on, you are prompted to change your initial password (if you have not already done so) and register the appliance with Websense blueSKY. See *Registering the appliance* for information.

> **Note**
> If you are unable to access the appliance, you can connect to the appliance manager interface at any time using the C1 interface via https://169.254.0.2.

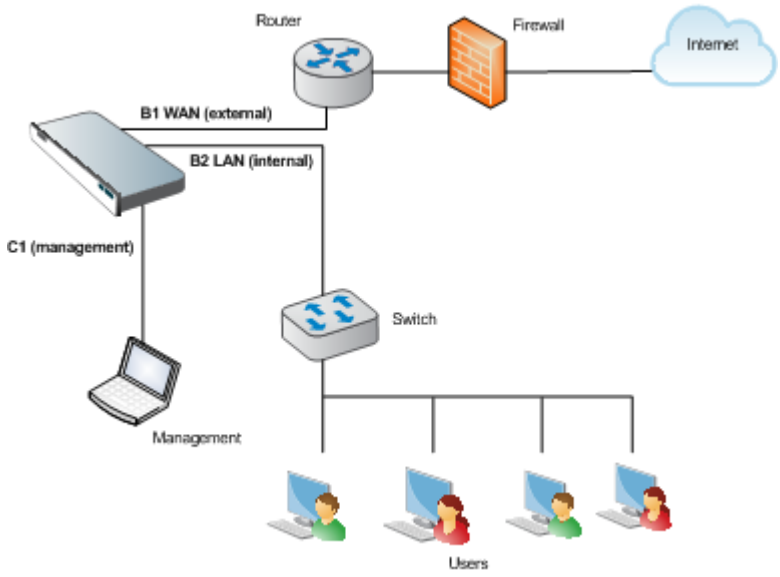
Connecting the appliance to your network

Getting Started Guide | Websense blueSKY Security Gateway

Connect the appliance to your network. The appliance must have at least a valid connection to the cloud service for registration and the subsequent initial database download to succeed. You can choose either of the following methods:

- Install the appliance in your network and then register it with the cloud service. The appliance operates as a simple network bridge, forwarding all traffic, until registration is complete.
- Install the appliance offline, with only the B1 interface connected to the network to allow an upstream connection to the cloud service. Once registration is complete and the appliance is fully set up, you can connect it to your the rest of your network.

The sample diagram shows a possible deployment:



Configuring your firewall

If your network includes a firewall, by default your appliance is configured to use the standard destination TCP ports 80 and 443 for connections to the cloud service. Ensure these ports are open.

Alternatively and depending on your corporate firewall policy, you can configure your appliance to use the following ports, which are the ones 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 appliance to retrieve periodic configuration and policy updates from the cloud service.
8081	**Proxy service**. This is where the 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). This port should also be opened for standard web traffic that does not need to be sent to the cloud for further analysis.
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. This port should also be opened for standard secure web traffic that does not need to be sent to the cloud for further analysis, and for database updates.

You can switch between the standard and alternative ports at any time using the appliance command-line interface (CLI). To switch port settings:

1. On the appliance machine, open a command-line window.
2. Type **device**.

   ```
   cmd> device
   ```
3. Type one of the following:

   ```
   device> use_standard_ports yes
   ```

   for the standard ports 80 and 443

   ```
   device> use_standard_ports no
   ```

   for the alternative ports 8002 and 8081, plus 80 and 443

   The CLI returns the confirmation `Done` when the ports have been switched. If the ports are already set to the option you specify, the CLI returns `Not changed`.

You must also open outbound UDP port 123 to enable the appliance to synchronize its clock with the Network Time Protocol.

To guarantee availability, Websense blueSKY uses the Websense global load balancing technology to direct traffic across multiple geographic locations. Content

analysis is typically always performed by proxies from the Websense cloud service closest to the end user. In the event of localized or Internet-wide connectivity issues, the Websense global load balancing technology automatically routes requests to the next closest location. To make the most of the resilience offered by this infrastructure, users must be allowed to connect to the entire Websense cloud service network - those IP addresses that the service uses now and those that may be deployed in the future.

If you decide to lock down your firewall, you should permit all the IP address ranges in use by the Websense cloud service for all the above ports. These ranges are published in a Knowledge Base article called "Cloud Service cluster IP addresses and port numbers." Note that you need to log on to MyWebsense to view this article.

Registering the appliance

Getting Started Guide | Websense blueSKY Security Gateway

In order to manage your appliance, you must register the appliance with Websense blueSKY.

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 Websense blueSKY registration key. 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 appears on the **Status > General** page. This message disappears when the initial download is complete.

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

Configuring Active Directory authentication

Getting Started Guide | Websense blueSKY Security Gateway

Use the appliance **Configuration > System** page to connect to an Active Directory server for transparent NTLM authentication. When this screen first opens, the status under Active Directory Authentication is **Disconnected**, and a button labeled **Connect** is available.

To establish a connection to an Active Directory server for authentication:

1. Click **Connect**.
2. In the Active Directory Authentication dialog, enter the following server information in the appropriate fields:
   - Domain name
   - Administrator name
   - Password

     Note that this password is used only for establishing the server connection. The contents of this field are not stored anywhere in the system.
3. Indicate how the system finds the domain controller by selecting 1 of the following options:
   - Auto-detect using DNS
   - Enter a domain controller name or IP address.

     You can specify backup servers in a comma-separated list.
4. Click **OK**.

The connection cannot be made if the server hostname does not adhere to Active Directory naming restrictions. See *First-Time Configuration Wizard*, page 14, for a detailed list of Active Directory hostname requirements.

After a connection is successfully established, the button name changes from **Connect** to **Disconnect**.

Running diagnostics

The Diagnostics tab on the appliance **Status > Alerts and Diagnostics** page provides the capability to run a series of system tests to determine the current state of Websense blueSKY Security Gateway. As a best practice, it is recommended that you run these tests when you first deploy an appliance, and if you encounter any connectivity issues.

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 results of the last test run appear, along with the date/time of those tests.

4 Setting Up End-User Authentication

The Websense blueSKY service works “out of the box” for many organizations. A single policy applied to an organization’s Web traffic provides protection from malware and inappropriate content. Most companies, however, want to tailor the service to align it with their Internet usage policy, which may require granular configuration on a per-user and per-group basis. Also companies usually want to report on the surfing habits of their employees, which requires users to identify themselves.

Authentication and identification options are set up on the Access Control tab within your policy. Log on to the cloud portal, go to **Web Security** > **Policy Management** > **Policies**, click your policy name, then select **Access Control**.

End-user authentication options

If forced authentication is configured in the policy, end users can use the details entered during registration to authenticate with Websense blueSKY whenever they access the Internet.

For secure form-based authentication, users are asked to authenticate the first time they open a browser. Users who have authenticated once do not then have to re-authenticate for subsequent Web browsing sessions, for a period of time defined by the Session Timeout option on the Authentication tab for the appliance in the cloud portal.

For basic authentication, users are asked to authenticate when opening a new browser instance. Once authenticated, they are not asked to authenticate again for the period of time defined by the Session Timeout option on the Authentication tab.

Enabling browsers for NTLM transparent authentication

NTLM transparent authentication is available for your end users if:

- you have chosen to connect your appliance to a local Active Directory, or you entered your NTLM domain on the Authentication tab when you added your appliance to Websense blueSKY.
- you select **NTLM transparent identification where possible** on the Access Control tab in your Websense blueSKY policy.

> **Note**
> If validating against a local Active Directory for NTLM authentication, an end user cannot use their email addresses as their user name, and must use the domain\username format (for example, MYCOMPANY\jsmith).

You must also configure your end users' browsers to support this form of authentication. In order for a browser to work with NTLM transparent authentication, the machine on which the browser is hosted must be part of the domain.

This section describes how to configure supported browsers, either manually or via a Group Policy.

Configuring Internet Explorer

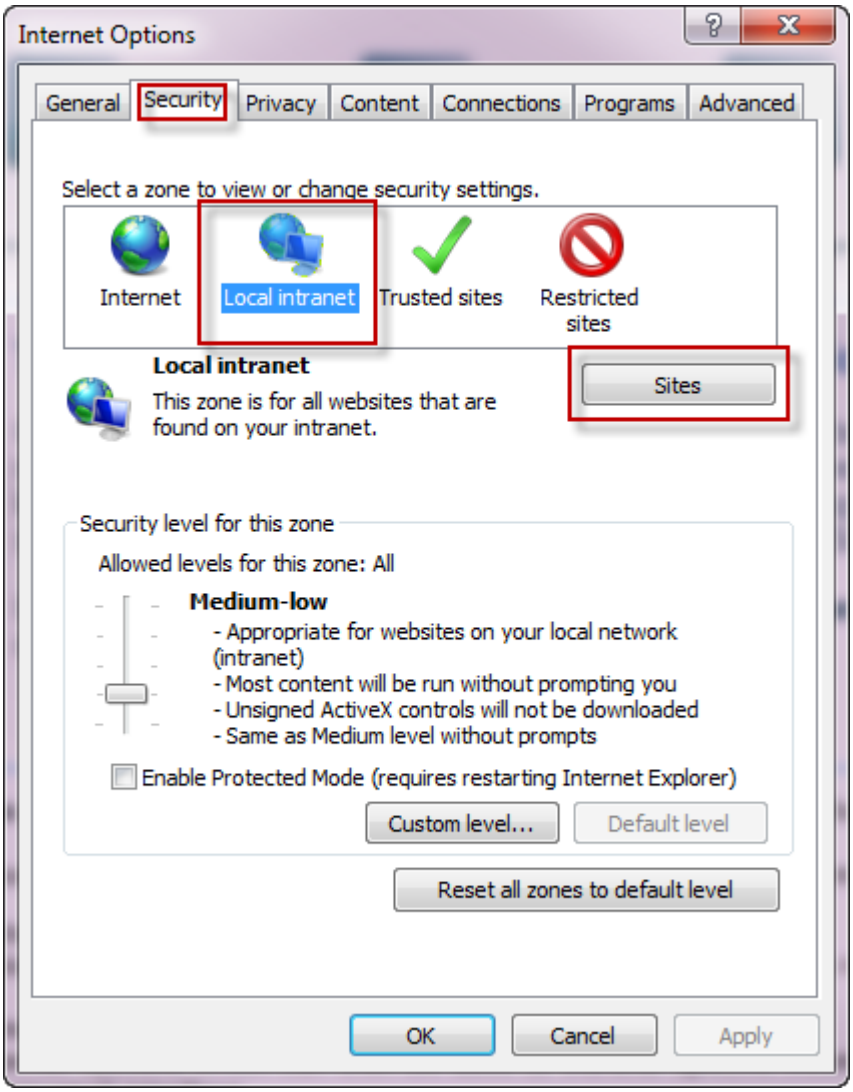
Getting Started Guide | Websense blueSKY Security Gateway

> **Note**
> The settings in this section will also be applied to a Google Chrome browser on the same machine.

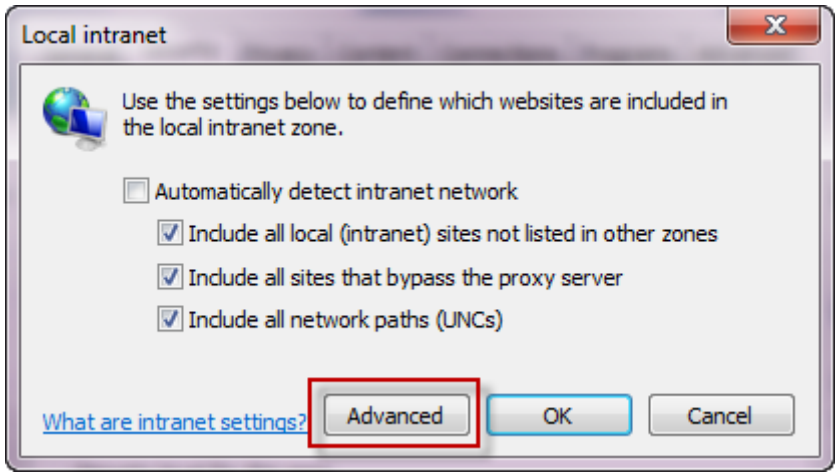
To enable NTLM on a single Internet Explorer browser:

1. Go to **Tools > Internet Options**.
2. Select the **Security** tab.

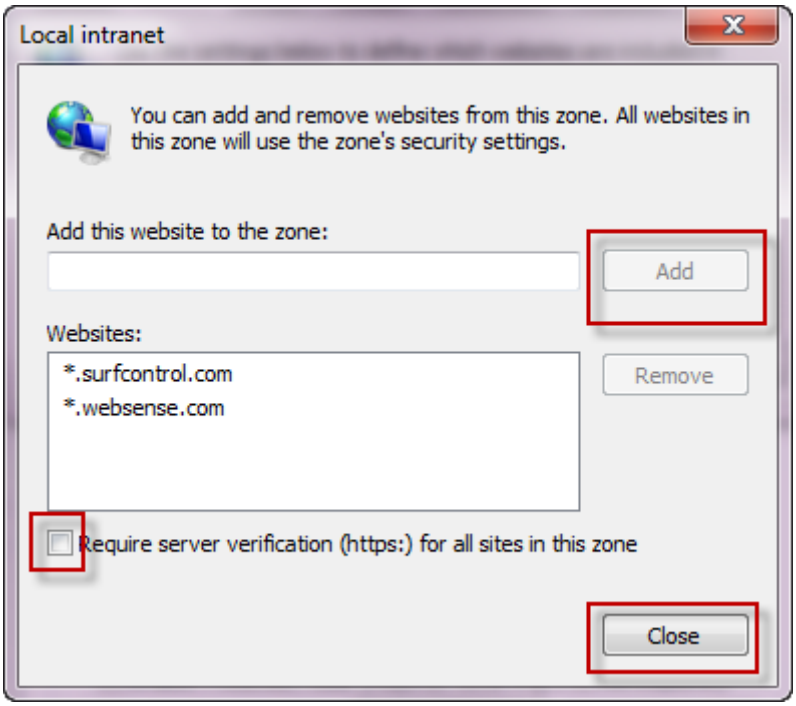
3. Select **Local Intranet**, then click **Sites** to open the list of Trusted Sites for the Intranet zone.



4. For Internet Explorer 8 and above, click **Advanced** on the window that appears. This step is not required for Internet Explorer versions 6 and 7.

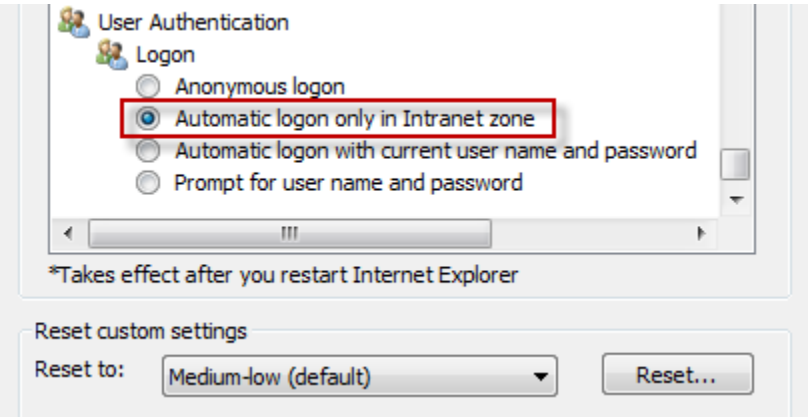


5. Enter the IP address of the B1/B2 bridge interface on your appliance, then click **Add**.
6. Clear the **Require server verification** box.
7. Click **Close**.



8. With Local Intranet still selected, click **Custom level**.

9. Scroll down to the User Authentication section, and ensure **Automatic logon only in Intranet zone** is selected.



10. Click **OK**, and exit Internet Options.

Configuring NTLM via Group Policy

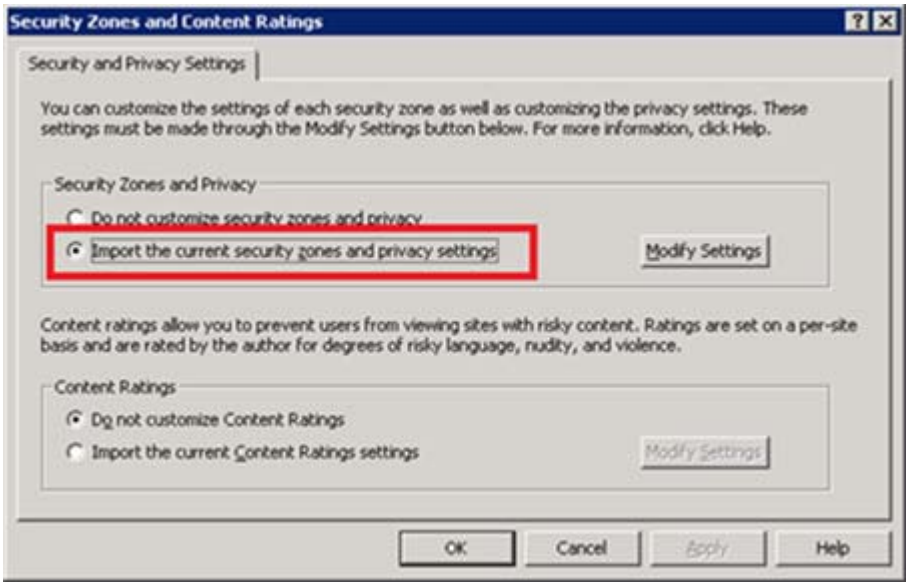
Getting Started Guide | Websense blueSKY Security Gateway

To create an NTLM transparent authentication policy using a Group Policy Object (GPO):

1. Log on to your Active Directory domain controller (DC) using a domain admin account.
2. Perform the steps listed in *Configuring Internet Explorer* to enable NTLM in the Internet Explorer or Chrome browser on the DC.
3. Turn off Internet Explorer Enhanced Security Configuration as follows (these steps apply to a Windows 2008 server):
   a. Open Server Manager.
   b. Scroll down to Security Information, and click **Configure IE ESC**.
   c. Turn ESC Off for administrators and users, and close the window.

4. Open Group Policy Management.
5. Right click your domain name (or the OU that contains the end users who will receive this policy), and click **Create a GPO in this domain, and link it here**.
6. Give your new policy a name, and click **OK**.
7. Right-click your newly-created policy, and select **Edit**.

8. Navigate to **User Configuration > Policies > Windows Settings > Internet Explorer Maintenance > Security > Security Zones and Content Ratings**.
9. Select **Import the current security zones and privacy settings**.



10. You may receive a warning about Enhanced Security Configuration. This is why the enhanced configuration was disabled in step 3, so that this policy will apply to workstations without enhanced security turned on. Click **Continue**.
11. Turn on Enhanced Security Configuration again, and repeat steps 4-9 to create a policy with ESC enabled. This ensures that workstations with either configuration are supported.
12. Close all open windows.

The changes will take time to replicate though your Active Directory, depending on your setup. This may be from 15 minutes to an hour; if you have a multi-site AD setup, it may take a day or two.

You can then set up a login script that will install the policy when end users log on to their workstations.

This method uses 2 files:

- login.bat
- ntlm.reg

The login.bat script contains two lines:

```
@echo off
regedit /s \\path\ntlm.reg
```

In the ntlm.reg script, replace <Box IP> with the IP address of your appliance:

```
Windows Registry Editor Version 5.00
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Internet Settings\ZoneMap\Ranges\Range5]
"*"=dword:00000001
 ":Range"="<Box IP>"
```

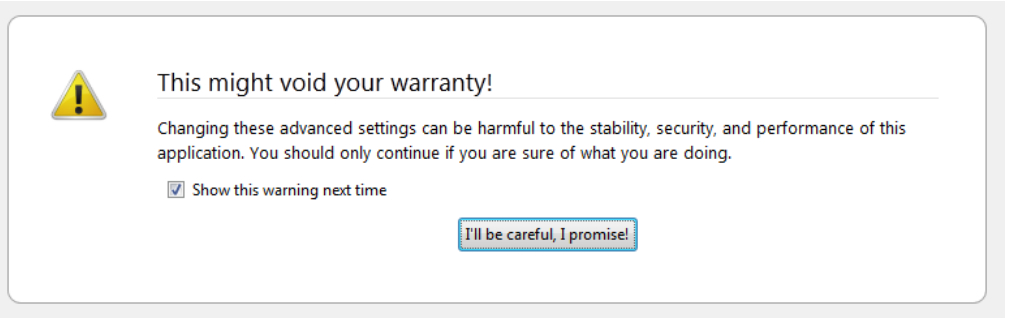
Configuring Firefox

Getting Started Guide | Websense blueSKY Security Gateway

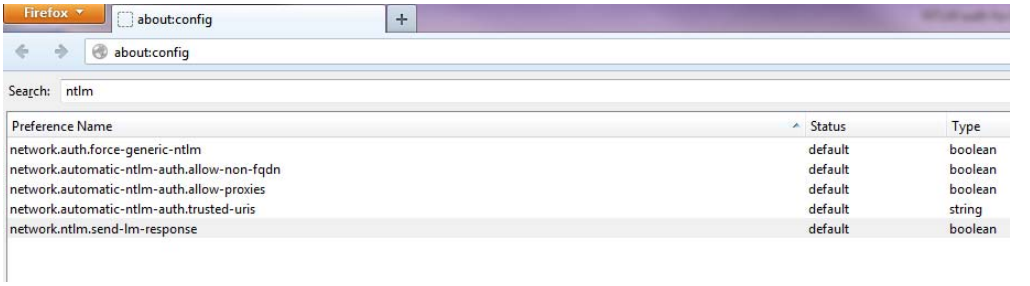
> **Note**
> If you are configuring Firefox v38 or later on Linux, you must perform step 6 in the procedure below to ensure the browser falls back to NTLM v1. This is due to the Linux version having issues with NTLM v2 that can cause authentication failures.

To enable NTLM transparent authentication in Firefox:

1. Open Firefox, and type about:config in the address bar.
2. Click **I'll be careful, I promise!** to open the advanced configuration page.



3. Type ntlm in the **Search** field.
4. Select **network.ntlm.send-lm-response** and double-click it to toggle it to on.



5. Double-click **network.automatic-ntlm-auth-trusted-uris**. In the box that appears, enter the IP address of the B1/B2 bridge interface on your appliance, and click **OK**.

6. If you are configuring Firefox on a Linux machine, double-click **network.auth.force-generic-ntlm-v1**.

   The Status is changed to **user set**, and the Value is changed to **true**.

End-user registration

Getting Started Guide | Websense blueSKY Security Gateway

If you do not use directory synchronization, the following options are available for end-user registration, and subsequent authentication or identification:

- *End-user self registration*
- *Bulk registering end-users*
- *NTLM transparent identification registration*

End-user self registration

Getting Started Guide | Websense blueSKY Security Gateway

One way to register users is to invite them to self-register. For those using secure form-based or manual authentication, there are 3 steps for individual end-user self registration:

1. You enter your email domains into the policy or account.
2. Users complete stage 1 registration (enter name and email address into a form).
3. Users complete stage 2 registration (create a password).

Users can access the stage 1 registration form at:

https://www.mailcontrol.com/enduser/reg/index.mhtml

or by clicking **Register** on the default pre-login welcome page or NTLM registration page that is presented when they are forced to identify or authenticate themselves.

Once users have entered their name and email address into the form, they receive an email from Websense blueSKY. This contains a link, that when clicked, takes them to a page where they can complete registration stage 2 by creating a password.

Bulk registering end-users

Getting Started Guide | Websense blueSKY Security Gateway

Bulk end-user registration simplifies the self-registration process by reducing it from 2 steps to 1. Rather than end users visiting the portal and entering their name and email address into a form, you upload all their names and addresses at once. End users automatically receive email notification once the bulk upload is finished. They can then click a link on the email they receive and create a password on the portal.

NTLM transparent identification registration

If you do not have an LDAP directory and your users are using NTLM transparent identification, an additional one-time step is required.

The first time these users send a request to Websense blueSKY, an NTLM registration form appears where they must enter their email address and password. Websense blueSKY associates these user credentials with the NTLM credentials automatically obtained from the browser. This association is saved and the user does not have to complete this step again.

Note

If you are using directory synchronization and have synchronized NTLM IDs, users are not prompted for this information. Only NTLM users who self-registered, were invited to register, or were bulk registered have to perform this step.

5 Next Steps

You should now be directing all Internet traffic through Websense blueSKYand be protected from Internet threats. Websense blueSKY works “out of the box,” but to get best use of its features, you probably want to tailor your policy. Specific areas of interest may be:

- Creating additional administrators to delegate responsibilities
- Adding internal or other trusted sites to your non-proxied destinations
- Adjusting the website category dispositions to suit the nature of your business
- Creating custom categories to allow whitelisting or blacklisting of specific websites
- Creating custom protocols to handle non-HTTP Internet traffic.
- Creating groups of users
- Creating exceptions to override category or protocol dispositions for specified users, groups, and times of day

Configuration advice for all of these features and others can be found in the Websense blueSKY Help.. Some basic steps for configuring your policy and managing reporting in the Websense blueSKY portal are outlined in the sections below.

Managing web categories

Websense blueSKY includes dozens of website categories. These categories are designed to help you apply policy to your organization’s web surfing. If a website has not previously been categorized, we assign it the category “Unknown”.

Click the **Web Categories** tab to configure the action you want Websense blueSKY to take when users try to access websites in each of the categories.

The category list on the Web Categories tab includes the **standard categories** provided by Websense, and any **custom categories** that you have defined on the **Policy Management > Custom Categories** page.

In the Standard Categories section, child categories are indented under their parent categories. Parent categories allow specific categories to be grouped by a more generic description. However, there is no hierarchical relationship between parent

categories and the child categories within them: you can set a filtering action for a parent category without it affecting the child category, and vice versa.

To edit the Web filtering action for a category:

1. Select a Web category from the category list.

   You can select a category directly from the list, or enter text in the search box to locate the category you want.

   To select multiple categories, use the **Shift** and/or **Ctrl** keys. You can also use the drop-down menu above the category list to select or deselect the following categories:

   - all categories
   - privacy categories
   - Web 2.0 categories

2. Select an **Action** for the category:

   - **Allow access** means that any website within the category is always accessible, regardless of whether it exists in another category that has the **Block access** action.
   - **Do not block** ensures that the site is not blocked under this rule, but if it also exists in another category that has an action of **Block access**, it is blocked under that category.
   - **Confirm** means that users receive a block page, asking them to confirm that the site is being accessed for business purposes. Clicking **Continue** enables the user to view the site and starts a timer. During the time period that you configure (10 minutes by default), the user can visit other sites in the confirmed category without receiving another block page. Once the time period ends, browsing to any other Confirm site results in another block page.
   - **Use Quota** means that users receive a block page, asking them whether to use quota time to view the site. If a user clicks **Use Quota Time**, he can view the site.

     Clicking Use Quota Time starts two timers: a quota session timer and a total quota allocation timer. The session length and total quota time available for each category depend on the options selected on the **General** tab.
   - **Block access** blocks access to Web sites in this category unless they exist in another category with a filtering action of **Allow access**. When a site is blocked, you can choose a notification page to be displayed.

3. To apply the setting to all categories within the selected category, mark **Apply to all sub-categories**.
4. Click **Save**.

Note

To ensure that notification pages appear for HTTPS sites, mark **Use Websense certificate to serve notifications for HTTPS pages** on the **Web Security > Policy Management > Block and Notification Pages** page.

SSL decryption

Getting Started Guide | Websense blueSKY Security Gateway

Click the **SSL Decryption** tab in the policy to enable SSL decryption and configure SSL analysis in elevated risk categories for your end users.

When you enable SSL decryption, SSL-encrypted traffic is decrypted, inspected, and then re-encrypted before it is sent to its destination. This enables the cloud proxy to serve the correct notification page to the user – for example, a block page if the SSL site is in a category that the end user is prevented from accessing.

To implement SSL decryption for your end users, you need a root certificate on each client machine that acts as a Certificate Authority for SSL requests to the cloud proxy.

To install the root certificate for your end users and enable notification pages for SSL sites:

1. On the SSL Decryption tab, click **Websense Root Certificate** and download the certificate to a location on your network. You can then deploy the certificate manually, using your preferred distribution method
2. Once the certificate has been deployed, return to this page and mark **Enable SSL decryption**.
3. Click **Submit**.

Managing protocols

Getting Started Guide | Websense blueSKY Security Gateway

Click the **Protocols** tab to manage how protocols, or non-HTTP Internet traffic, are handled by a policy.

The list of protocols appears in a 2-level tree display similar to that in the Categories tab. Protocol groups can be expanded to show the individual protocols within each group.

The list on the Protocols tab includes the standard protocols provided by Websense, and any custom protocols that you have defined on the **Policy Management** > **Protocols** page. The standard protocol groups are updated regularly.

Configure how a protocol is filtered by selecting it in the protocols tree and specifying an action (**Allow** or **Block**) from the box on the right. You can select a protocol directly from the list, or enter text in the search box to locate the protocol you want.

Use the **Shift** and/or **Ctrl** keys to select multiple protocols.

Managing exceptions

Getting Started Guide | Websense blueSKY Security Gateway

Exceptions allow the default action for a Web category or protocol to be overridden for specified users and groups of users. Exceptions are listed at the bottom of the **Protocols** and **Web Categories** tabs. Click a protocol or category to view exception rules that may apply to it.

Click **Add** to add a new exception.

Reporting

Getting Started Guide | Websense blueSKY Security Gateway

The available reports for web traffic and analysis are located in the navigation pane under **Web Security > Reports**. Click a reporting category to see the options available in that category. Initially you can access only the **Selection** tab to enter selection criteria. Once you have generated a report, you can click the **Chart** and **Table** tabs to view the results in chart or table form.

For most reports, you can select filtering criteria that restricts the report results. Next to each of the filtering criteria is a note describing in more detail how to use that option.

Once you have decided on the report and the appropriate criteria, click **Generate report**. You may receive feedback at this point advising that the report might take some time to generate. Typically this is due to the amount of data that must be searched. You can often avoid this by adding more criteria to narrow the search. Click **Back** if you want to cancel the report.

Important

For IP address filtering in a browsing time, real time analysis, or volume report, traffic that is analyzed by the appliance is logged with the individual user's IP address. Traffic that is analyzed by Websense blueSKY is logged with the IP address of the network gateway. As a result, filtering by IP address should be carefully defined in order to produce an accurate report.

You can also do the following:

- Download the majority of report results as a comma-separated values (CSV) file or as a PDF file.
- Save the reports you generate most frequently and want to be able to locate quickly.

- Schedule one or more saved reports for regular delivery in HTML, PDF, or CSV format.

For more information about reporting and the full list of available reports, see the Websense blueSKY Help.