



Websense® blueSKY™ Help

Websense blueSKY Security Gateway

©1996–2014, Websense, Inc.
All rights reserved.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA
Published 2014

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense Inc.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Websense, the Websense Logo, Threatseeker and the YES! Logo are registered trademarks of Websense, Inc. in the United States and/or other countries. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows NT, Windows Server, Internet Explorer, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Contents

Chapter 1	Getting Started	1
	Logging on and portal security	1
	Privacy statement	2
	Idle timeout	2
	Customizable landing page	2
	Navigation	2
	Dashboard	5
	Alerts	6
	Licenses	7
	Further Information	8
Chapter 2	Setting Up Your Account	11
	Contacts	12
	Permissions	12
	Password settings	14
	Groups	18
	Downloading and uploading groups	19
	Directory Synchronization	19
	End Users	20
	Privacy protection	20
	Important rules for configuring accounts	21
Chapter 3	Working with LDAP Directories	23
	Web Security	23
	What is LDAP?	24
	How the service works with LDAP	24
	Planning for your first synchronization	26
	Deciding what to synchronize	27
	Basic steps	29
	On the portal	29
	On the client	29
	Portal tasks	30
	Configure directory synchronization	30
	Set up authentication	33

	Client tasks	33
	Maintenance	34
	View and manage user data.	34
	Assign a group to a different policy.	35
	View and print reports.	36
	View recent synchronizations	36
	Restore directories.	37
	Troubleshoot synchronization failures	38
	Turn off directory synchronization	39
Chapter 4	Configuring Web Security	41
	Custom categories	41
	Protocols.	43
	Adding a custom protocol	43
	Editing a custom protocol	44
	Block and notification pages	44
	Default notification page settings	45
	Editing notification pages	47
	Language support	50
	Time periods.	51
	Domains	52
	Policy-level domains	52
	Account-level domains	53
	Editing a domain	54
	Permissions implications.	54
	Legal requirements	55
	Full traffic logging	55
	Bypass settings	56
	Bypassing authentication settings	56
	Bypassing certificate verification	58
Chapter 5	Managing Network Devices	61
	Adding an appliance	62
	Registering an appliance	65
	Changing the appliance password.	65
	Viewing appliance properties and statistics	66
	Viewing alerts	67
	Deleting an appliance	67
Chapter 6	Defining Web Policies.	69
	General tab	70

Policy name	71
Administrator email	71
Policy template	71
Time zone	71
Internet availability	72
Full traffic logging	72
Confirm timeout	72
Quota time	72
Search filtering	73
User and group exceptions for time-based access control	73
Connections tab	74
Proxied connections	74
Non-proxied destinations	75
Access Control tab	75
Pre-logon welcome page	76
NTLM identification	77
NTLM registration page	77
End Users tab	79
Registering by invitation	80
Bulk registering end users	81
End user self-registration	82
Directory synchronization	83
NTLM transparent identification	84
Editing end-user registration pages	85
Managing registered users	85
Rules for policy association during end-user registration	85
Web Categories tab	87
Managing categories and filtering actions	87
Filtering actions	88
Using quota time to limit Internet access	90
Exceptions	90
Filtering action order	92
Category list	92
Protocols tab	93
Protocol exceptions	94
Application Control tab	95
Application control exceptions	96
File Blocking tab	97
Blocking by file extension	98
Web Content & Security tab	99

	Advanced analysis using real-time classification	100
	Antivirus file analysis	101
	Executable file analysis.	103
	Analysis exceptions.	103
	SSL Decryption tab	104
	Enabling SSL decryption	105
	Configuring SSL decryption for web categories.	105
	Bypassing SSL decryption for specific sites.	106
Chapter 7	Reporting.	107
	Reporting periods	108
	Downloading report results	108
	Downloading a CSV file	109
	Downloading a PDF file	109
	Account Summary report	109
	Scheduling Account Summary reports	109
	Printing Account Summary reports.	110
	Viewing detailed information	110
	Categorized reports.	111
	Report results	112
	Drilling down	112
	Saving reports	112
	Scheduling categorized reports	113
	Cloud Service reports	114
	Directory synchronization reports.	114
	Browse Time reports	116
	Web reports	116
	Application Control reports.	117
	Browsing Times reports	118
	Real-Time Analysis reports.	119
	Volumes reports	120
Chapter 8	Audit Trails	123
	Configuration audit trail	123
Chapter 9	Standard Web Configuration	125
Appendix A	Checklists for Setting up LDAP in Various Use Cases	129
	New Web and/or email customers	129
	Synchronizing users/groups with a single Web policy and exceptions	129
	Synchronizing users/groups with more than one Web policy, and planning to manage Web policy assignment through an LDAP directory.	130

Existing Web and/or email customers 131

- Wanting to manage users/groups from an LDAP directory 132
- Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal 133

Considerations for existing customers 134

1

Getting Started

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

This guide is intended for IT administrators who are responsible for setting up and operating Websense blueSKY accounts.

Websense blueSKY provides on-premises URL analysis and application/protocol detection for Web traffic, 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 analytics are applied and policy is enforced.

You configure and manage services in the cloud using the Websense blueSKY portal. The portal provides a central, graphical interface to the general configuration, policy management, and reporting functions of your cloud-based service, making defining and enforcing Web security an easy, straightforward process. You maintain control over the system through on-demand statistics and reporting.

Logging on and portal security

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions



Note

To use the Websense blueSKY portal, your browser must be Javascript-enabled.

Websense blueSKY is configured using the cloud portal.

The logon process uses cookies where possible. For the best user experience, we recommend that you accept cookies from the Websense blueSKY portal. If your Web browser is unable to, or is configured not to accept cookies from the portal, an additional screen appears during logon reminding you of the benefits of securing your session.

If the portal cannot use cookies to secure the session, it falls back to ensuring that all requests for the session come from the same IP address. This may cause problems for you if your company has several load-balanced Web proxies, because the portal perceives requests coming from several sources as a security breach. Companies with a single Web proxy or a cooperating Web proxy farm should not be affected.

To avoid problems, we recommend enabling cookies on your Web browsers.

Privacy statement

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

The portal uses 2 cookies during logon. The first is used to identify whether the user's Web browser is willing to accept and store cookies for the portal; it contains no information. If the first cookie is successfully stored, a second cookie is stored containing temporary information about the session. No personal information is stored in either cookie, and both cookies are used only for the duration of the session.

Idle timeout

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

For security reasons, if you are logged on to your Websense blueSKY account and are inactive for a pre-defined period, you are automatically logged off. When you next attempt to perform an action, you are asked to log on again. Once you have done so, you are taken to the area of the portal that you requested. The inactivity timer is between 30 and 60 minutes.

Customizable landing page

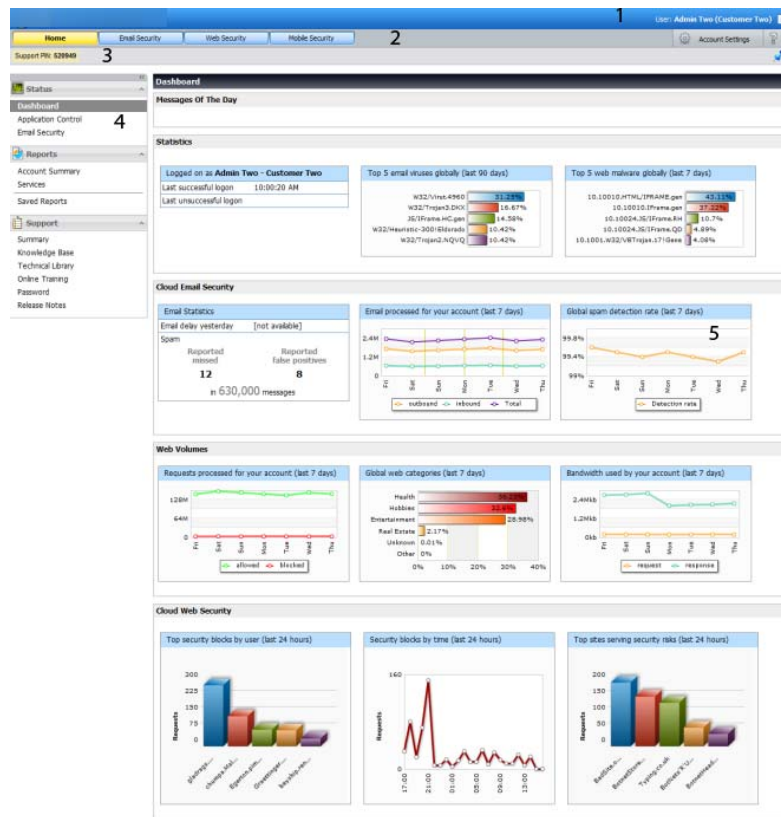
Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

By default, when you first log on to the portal, you land on the Support page. You can change your landing page by navigating to what you would like your landing page to be and clicking the **Pin** option in the top right of the page. Note that some pages have been deliberately excluded from supporting this functionality.

Navigation

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

The Websense blueSKY portal interface can be divided into 5 main areas:



1. Banner
2. Toolbar
3. Support PIN
4. Navigation pane
5. Content pane

The **banner** shows:

- ◆ Your current **logon account**
- ◆ A **Log Off** button, for when you're ready to end your administrative session
- ◆ Any **Alerts** that are available for your account

The **toolbar** indicates which part of Websense blueSKY is currently active:

- ◆ **Home** includes the *Dashboard*, access to Help and Support information, and access to reports that apply to the whole service
- ◆ **Web Security** contains all configuration settings relating to Websense blueSKY including account-wide Web settings, policy management, and Web reports.
- ◆ **Network Devices** lets you manage the devices in your network that connect to the cloud service.

- ◆ **Account Settings** provides access to configuration options that apply to all cloud service products. This includes Contacts, Directory Synchronization, licenses, and groups.

It also provides access to **Help** for the page you are currently viewing.

The button for the current active module in the toolbar is yellow. Buttons for modules that are available but not currently active are blue.

The **Support PIN** is always visible in the portal. You must authenticate yourself with this PIN when calling Websense Technical Support.

Each PIN is unique per portal user, and is generated when a user logs on. The PIN is then valid for 24 hours after logon. After a 24-hour period has expired, a new PIN is generated at the next portal logon.



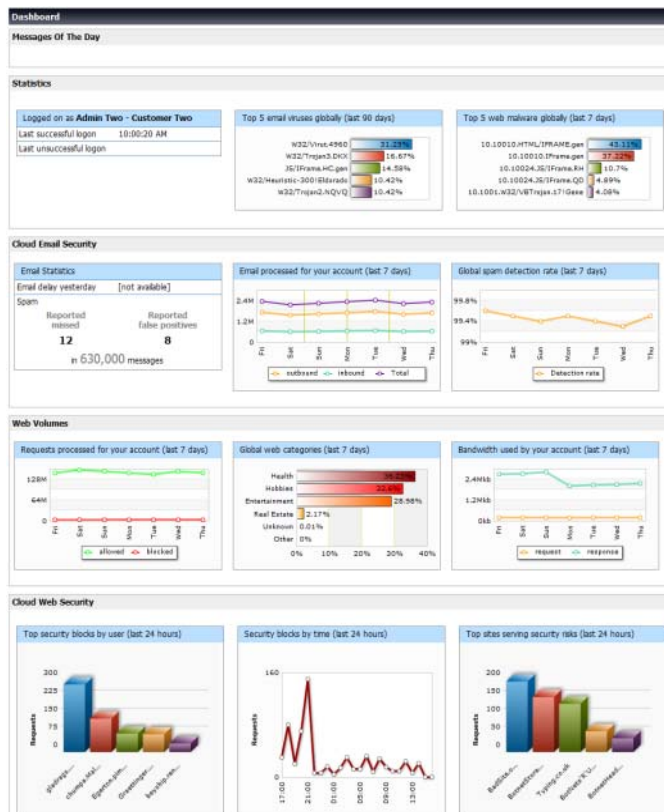
Important

In order to preserve and maintain the security of your data, Support representatives will not be able to provide customer support without an accurate, up-to-date PIN.

The **navigation pane** contains the available navigation choices for the service or configuration option that is currently selected. The **content pane** varies according to the selection in the navigation pane.

Dashboard

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions



The portal includes a dashboard that shows a summary of your account. To view your dashboard, go to **Home > Status > Dashboard**. The dashboard provides a snapshot view of how your Websense blueSKY services are performing.

The panels you see depend on your subscription settings.

Significant settings to note are:

- ◆ Details of your last successful and unsuccessful logons.
- ◆ The number of days until your license expires. Displays when less than 28 days.
- ◆ A list of the top current email viruses and Web malware globally in the last 7 days.

Below this are 3 charts summarizing volume statistics for your Websense blueSKY account in the last 7 days:

- ◆ Number of requests processed for your account. The allowed and blocked requests are shown in green and red respectively.
- ◆ Request composition - this categorizes the websites visited.
- ◆ Bandwidth used by your account. The outbound (requests) and inbound (response) traffic are totaled separately.

Three additional charts show Web security-related information for your account over the last 24 hours:

- ◆ Top five users by number of blocked requests in descending order.
- ◆ Number of requests blocked by time of day.
- ◆ Top five websites serving the most security risks and the number of requests made to access these sites in descending order.

Application Controls dashboard

To view a snapshot of how application controls are working, go to **Home > Status > Application Controls**. This dashboard provides the following charts:

- ◆ Major application types accessed over the last 7 days. This shows the number of times sites like Facebook, LinkedIn and Twitter have been accessed by end users.
- ◆ Facebook over the last 7 days – shows how often particular application controls were accessed on Facebook.
- ◆ Twitter over the last 7 days – shows how often particular application controls were accessed on Twitter.
- ◆ LinkedIn over the last 7 days – shows how often particular application controls were accessed on LinkedIn.



Alerts



Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Click the speech bubble icon in the Websense blueSKY toolbar to see alerts for your account.

Alerts are the primary means of communicating with customers to keep you fully informed of service issues. If you suspect that there may be a problem with the service, log on and check for new alerts. The number of alerts for your account is displayed with the alert icon.

You may see the following alert types:

	Error. Your service has been interrupted, and you must act on this alert immediately.
	Severe. You must act on this alert as soon as possible. If you do not act by the date given in the alert, it will be upgraded to Error and you risk interruption of your service.

	<p>Warning. This alerts you to future events that might affect your service – for example portal outages, or license expiration.</p>
	<p>Information. This might be announcing a new release or upcoming maintenance work.</p>

Select an alert summary in the left pane to see more detail, if available, in the right pane.

Licenses

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Our subscription model operates in a similar manner to many software vendors: to use the service, you must accept the terms of your agreement. Once you have done this, your services are automatically enabled, renewed, or upgraded depending upon the subscription type.

The Websense blueSKY purchase and billing systems are fully integrated with the portal. Each service has a subscription associated with it, and that subscription is applied to each customer account.

To view the subscriptions associated with your account, go to **Account Settings > Licenses**. You can use this area of the portal to view and manage your rights to use Websense blueSKY services.



Note

If an alert indicates that your account is currently unlicensed, please check the **Licenses** screen for further information.

Licenses screen

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

The **Licenses** screen provides basic information about your account. Depending on the subscriptions associated with your account, you may see up to 3 sections:

1. Pending licenses: Licenses that require accepting.
2. Current licenses: Licenses that have been accepted and are currently valid.
3. Previous licenses: Licenses that have either expired or been replaced by another license.

License information

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Subscriptions are generated automatically when you order a service. Each subscription contains the following information:

- ◆ **Contract:** The contract governing the license. This contains a link to a copy of the contract.
- ◆ **License type:** This provides information about the type of subscription (renewal, upgrade, etc.) and the contract type (for example, evaluation, SIB).
- ◆ **Services:** The services that your account is licensed to use.
- ◆ **Users:** The number of users or mailboxes for which your account is licensed.
- ◆ **Ordered by:** The name of the reseller that ordered the license for you.
- ◆ **Valid from / until:** Start and end dates of the license.
- ◆ **Billing period:** When you pay for your license – typically annual in advance or multi-year in advance.

Accepting licenses

WebSense blueSKY Security Gateway Help | Cloud Web Security Solutions

The first time you log on to a new WebSense blueSKY account, you are shown the licenses screen and must accept the terms of the agreement to activate your account and continue. If multiple subscriptions exist, you can accept them all at once.

Whenever a new subscription is ordered for you (for example, at renewal time or following an upgrade), it is added to your account in a pending state. You must accept this subscription to use the service. Each time you log on, you are taken to the licenses screen to remind you that a subscription requires accepting.



Note

To ensure continuity of service, you should accept any pending licenses as soon as possible. This requires Modify Configuration permissions.

If your license expires before you have a chance to renew it, you receive a grace period. During that period, please order a new subscription as soon as possible.

Further Information

WebSense blueSKY Security Gateway Help | Cloud Web Security Solutions

The **Home > Support** section of the portal is your resource for further information about WebSense blueSKY . This area of the portal provides access to the following resources:

How to get Support

The **Home > Support > Summary** page provides you with a link to Product Support. We ask that you take a few minutes to review the material available through the Support pages first, to see if your question has already been answered.

Password Maintenance

Go to **Home > Support > Password** if you need to change your password or generate a new one. Enter and confirm a password, then click **Submit** when done. The password must conform to your password policy, as described on the screen. See [Changing passwords](#), page 17 for more information about passwords.

Manuals

Several manuals are available. For administrators:

- ◆ This guide (*Websense blueSKY Help*)
- ◆ *Websense blueSKY Getting Started Guide*
- ◆ *Directory Synchronization Client Administrator's Guide*

Release Notes

Release notes contain the very latest information about the services. These list all new features, functionality, and fixes that are deployed with a new release and we recommend that you read them as soon as possible after a release so that you can take advantage of the new features.

2

Setting Up Your Account

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Click **Account Settings** in the Websense blueSKY toolbar to set up your account. On the resulting screen, you can control your account and the services you have purchased. You can:

- ◆ manage users who log on to the portal (also known as contacts)
- ◆ define groups of people who use the services
- ◆ view changes made to your settings in the Audit Trail
- ◆ configure your account for directory synchronization
- ◆ manage end users (web or directory synchronization only)
- ◆ define privacy protection settings (web only)

The Account Settings screen shows the configuration options that apply to the complete account.

To view the configuration audit database for your account, choose [Audit Trails](#), page 123.

Choose [Contacts](#), page 12 to view and modify the contact details of people in your organization who administer, support, and pay for the services. The administrator contacts can be given logons to the portal and their permissions restricted as necessary. You can also use this page to modify your password settings.

Choose [Directory Synchronization](#), page 19 to configure directory synchronization for your account.

Choose [End Users](#), page 20 to search for end users so you can enable or disable their Web access, delete them, or change their policy assignments. (This option is available only to accounts enabled for directory synchronization.)

When you define [Groups](#), page 18, they are available in all your policies in all services. This allows you to define a consistent set of rules across the services for groups of end users.

This chapter covers the configuration of account-level options. To configure the majority of Web service options, click **Web Security** and select the appropriate setting type or policy.

Contacts

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Permissions](#)
- ◆ [Password settings](#)

The Account Management area displays the current requirements for passwords in your account, as well as any expiration limit. For more information, see [Password settings, page 14](#).

The contact information in the **Contacts** area is created with the details supplied during enrollment. The initial contact assumes the role of Company Master User and has the highest rights and privileges for your account. In this area of the portal, you can manage the contact list for your account. We use these contact details when we need to communicate with you. You can specify a variety of contact addresses and numbers for each contact, plus a call order that specifies the order in which we should call them. To add a new contact, click **Add**.



Note

If the contact also has logon privileges, you must enter an email address to enable them to use the password reset function, if required.



Note

It is your responsibility to administer the logon privileges for the contacts in your account, and to ensure access to the Websense blueSKY portal is maintained or protected as appropriate. You are also responsible for any actions taken by the users of the portal logons that you create.

Permissions

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

To assign logon privileges to the contact you just created, open it back up by clicking the name of the contact. In the User Name area, click the hyperlink in **No user name. Click here to add one**, or click the email address hyperlink in the User Name field. (By default, the email address is used as the contact's logon ID.)

A User screen appears, where you can give the user a password and define expiration and permissions.



Note

You can also access this screen by clicking the contact's logon ID on the main Contacts screen (the User Name column).

You can type a password for the user and confirm it. Alternatively, if you want to automatically generate a password that complies with the password policy, click **Create a password for me**. The password, which meets the stated password policy, populates into the Password field.

By default, all rights are assigned to the Company Master User - the first contact established on your account. When this user creates a new user, by default only the **View All Reports** permission is assigned to the new user. This is the minimum permission a user needs to be able to log on; it grants permissions over only the Reporting tab on the main menu bar.

We provide flexible users' rights so you can create a hierarchy of administrators. For example, much of the functionality accessed from the portal is useful for help desk agents to aid with problem isolation; but they do not necessarily require control over policy configuration.

**Note**

When the user first logs on to the portal, a screen is displayed giving them 8 days to select a password question from the list provided and enter an answer. This password question and answer is used if the user later forgets their password (see [Forgotten passwords, page 18](#)). If the user does not set a password question within the 8-day limit, they are forced to do so at their next logon.

Likewise, you should assign Directory Synchronization privileges to the contact you set up for the Directory Synchronization Client (see [Set up authentication, page 33](#)), but no-one else should need this privilege.

Permissions are granted at an account and policy level. This lets you create multiple policies, and administrators can control their own policy but no one else's.

To modify an administrator user's permissions, click **Advanced**.

**Note**

The **Advanced** button does not show for contacts with Manage Users permissions, because they are assumed to have maximum account-level permissions.

Permissions definitions

The following are account-level permissions:

- ◆ **Manage Users** - User can create, edit, and remove user logons and permissions.
- ◆ **Directory Synchronization** - User can synchronize an LDAP directory with the cloud service.
- ◆ **View All Reports** - User can run all reports associated with the licensed services.

The following Websense blueSKY permissions can be assigned at an account or policy level:

- ◆ **Modify Configuration** - User can modify all options within Account Settings except users' logons – for this, the user must have **Manage Users** permissions.

- ◆ **View Configuration** - User can view all configurations within Setup, but not make any changes.
- ◆ **View Configuration Audit Trail** - User can access and search the policy setup audit trail.
- ◆ **View Filtered Reports** - User can only view reports that can be filtered by the specified policy or policies. This option is not available if View All Reports is selected.



Note

The View Filtered Reports option may not be enabled in your account.

Users with any of these permissions can access the Websense blueSKY service non-policy-specific configuration options.



Note

If users are logged on to the portal when their permissions are changed, the changes do not take effect until they log off and then log on again.

Websense blueSKY administrators can also restrict reporting options with group filtering. If you select one or more groups under **Group Filtering for Cloud Web Reporting**, only the users in those groups are visible in the reports that this user can run. Group filtering can be combined with the View Filtered Reports option for a Web policy: for example, a user can view only reports that apply to the IT and Engineering groups in the Default policy.



Note

The **Group Filtering for Cloud Web Reporting** option may not be enabled in your account.

Password settings

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Password policy](#)
- ◆ [Password expiration limit](#)
- ◆ [Changing passwords](#)
- ◆ [Forgotten passwords](#)

Click **Account Settings > Contacts > Edit** to define password settings for your account. On this screen, you can define an expiration limit for your users and also set up the user lockout option. If you have more than one password policy (a policy that defines how “strong” your users’ passwords must be), you can also choose which

policy to use on this screen. Click **Update** when you're finished making your selections.

Note that you can override these settings for individual users on their permissions settings screen.

Password policy

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Password settings](#)
- ◆ [Password expiration limit](#)
- ◆ [Changing passwords](#)
- ◆ [Forgotten passwords](#)

A password policy defines how “strong” your users’ passwords are required to be. (A strong password is a secure password.) The password policy in the cloud portal sets the minimum length, maximum length, password history, sequence rules, and unique character rules of a user’s password.

Following are the minimum requirements:

Parameter	Default policy value
Minimum length	8
Maximum length	30
Password history size (number of former passwords to check)	3
Maximum number of characters in sequence	4
Minimum number of unique characters	5

In addition, passwords:

- ◆ cannot contain the user’s logon ID.
- ◆ cannot contain common words or keyboard sequences.
- ◆ must include uppercase letters.
- ◆ must include lowercase letters.
- ◆ must include numbers.

Password expiration limit

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Password policy](#)
- ◆ [Password settings](#)
- ◆ [Changing passwords](#)
- ◆ [Forgotten passwords](#)

We recommend that you force users to change their passwords on a regular basis. Passwords can be set to automatically expire in a set time period. You configure this on the main setup screen for the account. You can override this setting for individual users on their permissions settings screen.

1. Select **Account Settings > Contacts > Edit**.
2. From the **Password expiration limit** drop-down list, select one of the following from the expiration period: 30, 60, 90, 120, or 180 days, Custom days.

When you click **Custom days**, a new field appears so you can enter any number of days you want. Periods longer than 365 days are not supported.

3. Click **Update**.

User lockout

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Unlocking user accounts](#)
- ◆ [Changing passwords](#)
- ◆ [Forgotten passwords](#)

If a user enters an incorrect password when attempting to log on, they have a limited number of further attempts before they are locked out for a period of time. You set up the number of further attempts and the lockout time period on the main setup screen for the user.

1. Select **Account Settings > Contacts > Edit**.
2. From the **User lockout** drop-down list, select a lockout time period. The options are 15 minutes, 1 hour, 4 hours, 24 hours, or Forever.

If you select **Forever**, an administrator with Manage Users permissions must unlock the user account before the user can log on again.

3. Select the number of permitted failed attempts from the drop-down list. This can be between 3 and 10.
4. Click **Update**.

Unlocking user accounts

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [User lockout](#)
- ◆ [Changing passwords](#)
- ◆ [Forgotten passwords](#)

If a user is locked out because they failed to enter the correct password after the allotted number of attempts, an administrator with Manage Users permissions can unlock the user account before the lockout time period has ended. If the lockout time period is set to **Forever**, the user must be unlocked by an administrator.

1. Select **Account Settings > Contacts**.
2. In the User Name column of the contact list, click the required user name.
3. Click **Edit** on the User screen.
4. Click **Unlock**.
5. Click **Submit**.

Changing passwords

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Password policy](#)
- ◆ [Password settings](#)
- ◆ [Password expiration limit](#)
- ◆ [Forgotten passwords](#)

Users are required to change passwords when they expire or when a change is forced by an administrator. Only administrators with Manage Users permissions can force a user to change his or her password. To force a change, select the **Change Password next logon** box on the user's contact screen. When users are required to change their passwords, they see a Change Password screen the next time they log on.

Users can also opt to change their password from **Home > Support > Password**, which displays the same Change Password screen.

If a user creates a password that does not meet the password policy standards, they receive an error message and are asked to try again. For example:

This password has been used recently. Please try another.

To implement the changed password, users should click **Submit**. They should also make note of the password for future reference.

Forgotten passwords

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Password policy](#)
- ◆ [Password settings](#)
- ◆ [Password expiration limit](#)
- ◆ [Changing passwords](#)

If a user forgets their password, they can click the **Forgot your password?** link on the logon screen and follow the instructions to reset the password:

1. The user enters their portal user name and clicks **Submit**.
2. Websense blueSKY sends an email to the email address listed in the contact details associated with that user name.



Note

If the email address set up for the user name on the Contacts page is out of date or invalid, the user must contact their administrator to get their password reset.

3. The user clicks the link in the email to go to a secure page.
4. The user enters the answer to their password question, and clicks **Submit**.
5. When the question is answered correctly, the user can enter and confirm a new password. They also have the option to change their password question.



Note

If a user forgets the answer to their password question, they must contact their administrator to get their password reset.

Should you need to generate a new password for a user, follow these steps:

1. Select **Account Settings > Contacts**.
2. In the User Name column of the contact list, click the required user name.
3. Click **Edit** on the User screen.
4. Click **Create a password for me**.
5. Make note of the password.
6. Click **Submit**.

Groups

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Websense blueSKY supports groups functionality. This enables you to create policies using your organization's hierarchy.

Groups can contain:

- ◆ email addresses of users in your organization
- ◆ other groups

Groups are configured at the account level. To set up groups in Websense blueSKY, click **Account Settings > Groups**.

The resulting screen shows a list of groups currently defined for your account, an indication of whether they were added manually on the portal or automatically through the directory synchronization feature, and the Web policy to which the group is assigned.

On this screen, you have the ability to create new groups and edit group membership. Click a group name to edit it, or click **Add** to add a new group.



Important

Add or load groups only if you intend to use them for policy assignment or exceptions. You don't need them just because users are members of them.

Downloading and uploading groups

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

If you are managing groups strictly on the portal (in other words, you are *not* using directory synchronization), you have the option to upload or download a list of groups in a comma-separated values (CSV) file. You can then edit this using a simple text editor or a spreadsheet application such as Microsoft Excel.

Directory Synchronization

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Working with LDAP Directories](#)
- ◆ [What is LDAP?](#)
- ◆ [How the service works with LDAP](#)
- ◆ [Basic steps](#)

Click **Account Settings > Directory Synchronization** when you want to configure your account for directory synchronization. See [Configure directory synchronization, page 30](#) for details on this screen and other LDAP considerations.

End Users

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [End Users tab](#)
- ◆ [Managing registered users](#)

To view and manage user data, click **Account Settings > End Users**. (This option is only available if you have directory synchronization enabled.) The resulting screen has 3 columns.

Column	Description
Criteria to use	Check the boxes on the left to indicate what search criteria to use.
Search Criteria	Narrow down the search by entering or selecting precise data in the middle column. Under source, you can choose whether to search <i>synchronized</i> users or <i>portal-managed</i> users.
Show in Results	Check the boxes on the right to indicate what information to include in the results.

Click **Search** when done. Please note that the search may be slow if there are a large number of users.

From the resulting data, you can make individual edits or bulk edits. For example, you can:

1. Move user(s) to another Web policy, performing a manual override
2. Undo the manual override (applies only to directory synchronization)
3. Enable or disable user(s) Web access
4. Delete user(s)

Using the drop-down list between the search box and the search results, select the action you want to make, then select the users on which to perform the action and click **Go**. All changes made on this screen override any group/policy assignments (existing or future ones).

You can view and manage user data at the policy level as well using the **End Users** screen for the policy. The account-level page is available only to users with account-level privileges.

Privacy protection

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Use the **Account Settings > Privacy Protection** page to prevent end-user identifying information from appearing in logs and web reports.

End user identifying information comprises user names and IP addresses. If you want to prevent this information from appearing only for some of your end users, ensure those users are all registered to a specific policy or policies.

1. Select **Anonymize end user information**.
2. Define whether to anonymize user information in all policies, or only selected policies.

**Note**

If you select **All policies**, this applies to all existing policies and any new policies you create in the future.

3. If you choose **Only selected policies**, select the policies you want from the Available policies list. Use the **Ctrl** and/or **Shift** keys to make multiple selections.
4. Click the **>** button to move the policies into the Selected policies list.
5. Click **Save** when done.

Important rules for configuring accounts

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

- ◆ web It is good practice to keep the number of policies to a minimum, because if a global change is required, you must make it across all policies.
- ◆ To prevent accidental changes, many configuration options are greyed out until you click the appropriate edit box.
- ◆ Each service has its own configuration screen accessed by clicking the appropriate tab on the main policy setup screen. Regardless of the services that you are licensed to use, you see all tabs. If you click the tab for a service that you are not licensed to use, you are informed of such.
- ◆ Where multiple email addresses, domains, or user names are entered into a screen, they should be separated by commas.
- ◆ You can click **Help** at any time to access online help information.
- ◆ All changes are made in real time and usually only take a few minutes to propagate across the Websense blueSKY infrastructure.
- ◆ Websense blueSKY analyzes inbound and outbound web traffic as well. Most settings in the policy screens are specified separately for inbound and outbound policy application. It is often not appropriate to set these identically for each direction.

To access a web policy, click **Web Security**. Then go to **Policy Management > Policies**, and you are presented with a choice of service-specific policies.

3

Working with LDAP Directories

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Maintenance](#)
- ◆ [Configure directory synchronization](#)

Websense blueSKY allows you to make use of existing LDAP directories, such as Active Directory, so you don't have to recreate user accounts and groups for your email and Web services or manage users and groups in two places.

Although Websense blueSKY is a cloud-based service, it synchronizes with LDAP directories via a client-resident application known as 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.



Important

Websense blueSKY supports only one instance of the Directory Synchronization Client for each account. Using multiple synchronization configurations, or even using multiple installations of the Directory Synchronization Client, can cause data on the Websense blueSKY service to be overwritten.

Web Security

For Websense blueSKY, you can synchronize your end users using the Directory Synchronization Client. If you have set up the account for NTLM identification and synchronized NTLM IDs, end users do not need to register for the service on the portal (unless they are travelling outside of the network).

What is LDAP?

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [How the service works with LDAP](#)
- ◆ [Basic steps](#)
- ◆ [Portal tasks](#)
- ◆ [Client tasks](#)
- ◆ [Maintenance](#)
- ◆ [Configure directory synchronization](#)
- ◆ [Set up authentication](#)

Lightweight Directory Access Protocol (LDAP) is a networking protocol for querying and modifying directory services. An LDAP directory contains data with similar attributes and organizes data in a directory tree structure. It is considered “lightweight” because it is a reduced version of the X.500 directory standard.

Active Directory (AD) is Microsoft’s LDAP-compliant directory service, and is an integral part of the Windows Server architecture. Active Directory is a hierarchical framework of resources (such as printers), services (such as email), and users (user accounts and groups). It allows administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization.

Websense blueSKY integrates with LDAP directories and has been certified to work with Microsoft Active Directory. If you have enterprise information stored in AD, you do not have to enter it into the manually.

How the service works with LDAP

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

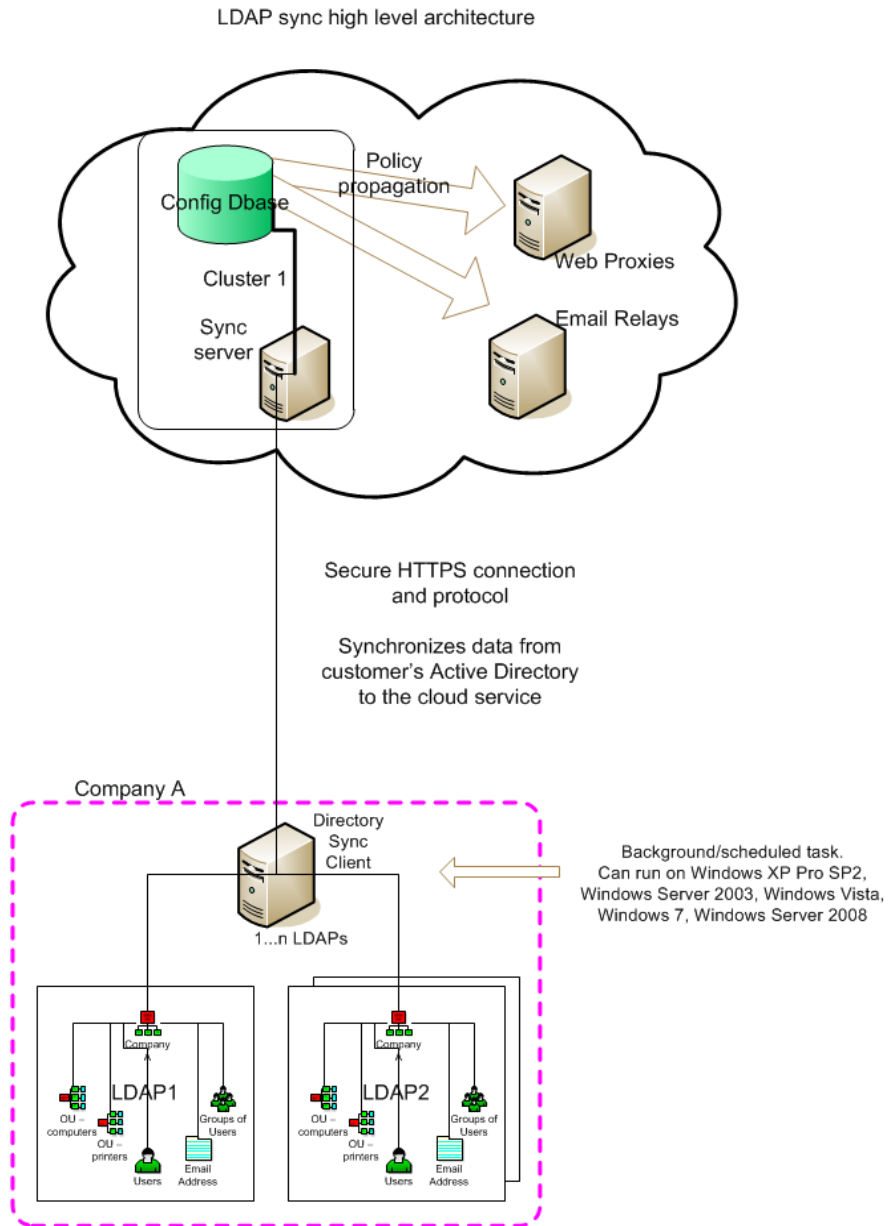
For each data synchronization:

1. The Directory Synchronization Client communicates with the LDAP server and returns the selected data (users, groups, and email addresses).
2. The Directory Synchronization Client performs a synchronization and returns incremental changes to the portal via Secure Hypertext Transfer Protocol (HTTPS). You can force a full synchronization when necessary.

3. The uploaded data is stored in the cloud service along with users and group data managed through the administrator portal.
4. If both user and group data is required, the update occurs in 2 transactions. If one fails, the other can still succeed. Email addresses are a third transaction.
5. The client authenticates with the portal using a username and password that you establish manually on the portal **Contacts** page. (Consider an appropriate password expiration policy for that user so you don't have to regularly update the client application with the password changes.)
6. LDAP synchronized data is viewable but not editable through the portal.

The synchronization client resides on a computer at the customer's site and accesses one or more LDAP directories via the customer's network. If more than one LDAP

directory is accessed, then this data can be merged together by the synchronization client before it is synchronized with the cloud-based service.



Planning for your first synchronization

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

When you are setting up directory synchronization, it is important that you review the data you are about to synchronize before you synchronize it. The way that you

structure data in your LDAP-compliant directory affects how you should structure groups and users on the portal for policies and exceptions. You should devise a synchronization strategy before you start.

To start, what data do you want to get out of your LDAP directory and what do you plan to do with it?

Second, how is that data organized?

Third, how do you need to structure users and groups on the portal to accommodate your security requirements?

In a typical directory, users are members of many groups. For example, users may be members of global groups like “All Sales;” they may be members of geographical groups like “London” or “New York;” and they may be members of a department such as “NY Telesales” and many others. When deciding on which groups to synchronize, select only groups that are going to be useful to the cloud service, typically for setting policy or group-based exceptions. See [Deciding what to synchronize, page 27](#) for more guidelines on this decision.

If you already have users and groups on the portal, then you’ll need to determine how and whether to adjust that structure to match the LDAP directory (or vice versa).

Following are the most common use cases. Follow the links to review considerations and checklists designed just for you.

- ◆ New Web and/or email customers:
 - [Synchronizing users/groups with a single Web policy and exceptions](#)
 - [Synchronizing users/groups with more than one Web policy, and planning to manage Web policy assignment through an LDAP directory](#)
- ◆ Existing Web and/or email customers:
 - [Wanting to manage users/groups from an LDAP directory](#)
 - [Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal](#)

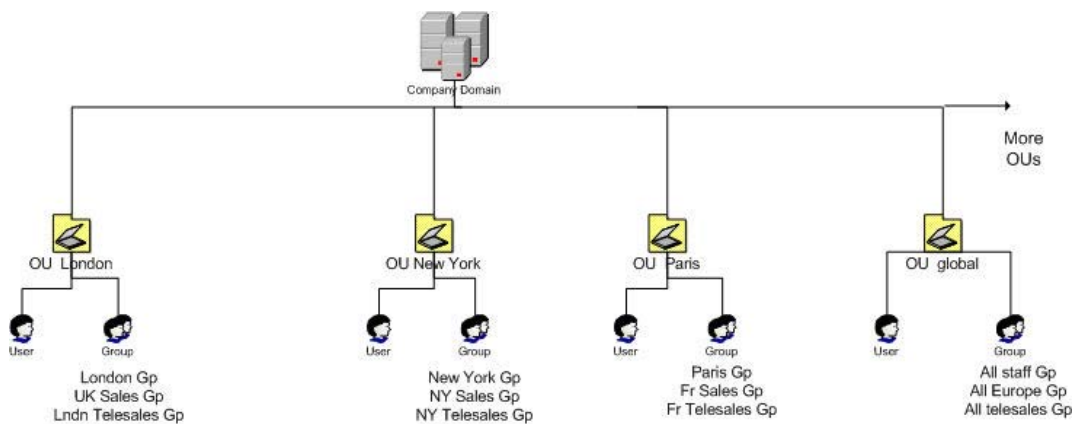
Deciding what to synchronize

Related topics:

- ◆ [What is LDAP?](#)
- ◆ [How the service works with LDAP](#)
- ◆ [Basic steps](#)
- ◆ [Portal tasks](#)
- ◆ [Client tasks](#)
- ◆ [Set up authentication](#)

You do not need to synchronize all of the groups and users in your LDAP-compliant directory. Instead, synchronize only groups that are useful to the cloud service.

Consider this Active Directory (AD) example:



If you are going to set up a policy for members of a New York Telesales department that gives them special permission to access certain Web sites, you should synchronize the “NY Telesales” group. There is no need to sync the “London” group if you are not going to set up geographical policies in the cloud service, even if the London users are going to be using the service.

Sometimes when users are synchronized to the cloud service, they are members of multiple AD groups, but only a subset of those groups is synchronized. This is not a problem: the cloud service is designed to accept users with group references that are not on the service.

You specify which groups to synchronize using an LDAP search facility on the Directory Synchronization Client. There is great flexibility in selecting the appropriate data to synchronize. For example, you can use the *membership of an LDAP group*

attribute to select the users you want, even though you may not select that group in the group synchronization setup itself.

**Note**

If you add or change a group name in Active Directory or move a group from one organizational unit (OU) to another, be sure to add the new name to the group inclusion list on the Directory Synchronization Client before the next synchronization. Otherwise, the group is deleted from the portal.

Regardless of how many groups you synchronize, user detail must be sent as part of a separate user synchronization. When you synchronize a group, you transfer information about the group but not about its contents. User synchronizations include details of the group(s) to which users belong. When you apply a Web policy or an email policy to a synchronized group, that policy is applied to all synchronized users who are members of that group.

Please refer to the [Directory Synchronization Client Administrator's Guide](#) in the Technical Library for more information on using the LDAP search feature to target only those users and groups that are required.

Basic steps

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Although the steps for your use case may vary, the basic steps for setting up directory synchronization follow:

On the portal

1. [Configure directory synchronization, page 30](#), for your account.
2. [Set up authentication, page 33](#), for the client machine. The client should have its own username and password to gain access to the cloud service.

On the client

1. Download the Directory Synchronization Client from the portal (see [Client tasks, page 33](#)) and install it on a network client machine. Download the client administrator's guide as well. This contains valuable information on helping you integrate your directory service with the .
2. Configure the client. Use the username and password established in the **Contacts** section of the portal to authenticate.

3. Test the Directory Synchronization Client to make sure it is returning the correct data from the LDAP server to the client. If you are an existing customer switching to directory synchronization for the first time, you should compare the data with that which already exists on the portal.
4. Initiate a synchronization. The service updates its groups and users, including policy assignment where appropriate.
If a synchronization is unsuccessful, you can use the **Restore** feature to restore the directory information to a previous version. (See [Restore directories](#), page 37 for more information.)
5. Schedule automatic synchronization. You can update the several times a day if required.

Refer to the [Directory Synchronization Client Administrator's Guide](#) for instructions on items 2-5.

Portal tasks

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Maintenance](#)

To set up your account for directory synchronization, perform the following steps on the cloud portal:

1. [Configure directory synchronization](#), page 30, for your account.
2. [Set up authentication](#), page 33, for the client machine.

Configure directory synchronization

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

1. On the main menu bar, click **Account Settings**.
2. Click **Directory Synchronization**.
3. Click **Edit**.
4. Check the **Enable directory synchronization** box. You cannot connect the Synchronization Client to the cloud server without doing so, even if you have a valid username and password.

5. Fill out the rest of this screen as follows:

General

Overwrite groups

If you are a new customer with no group data in the portal, leave this box unchecked.

If you have existing data and are migrating to LDAP, check this box if you want to overwrite current groups with the synchronized groups when there is a group name conflict.

Users, groups, and email addresses are overwritten by LDAP data of the same name. Once this occurs, they are manageable only by LDAP synchronization.

If you are switching to LDAP for the first time, take care to match your LDAP group names and membership to the existing setup. Doing so allows existing policy selections and settings to be maintained, as well as existing usernames/passwords where applicable.

If you have duplicate names, you have 2 options: make sure the duplicate can be overwritten or don't allow overwriting and rename the duplicates to avoid a conflict.

If you don't select this option and duplicate names are found, the transaction is rejected. On the portal, you receive the error "403: Attempt to overwrite portal-managed group 'nnnn'." On the client, you receive "Error communicating with the Hosted Service portal. Update abandoned."

Web

Assign users to policy	<p>Because you are synchronizing user and group data, you can manage policy membership through group membership.</p> <p>Select the Web security policy to which you want to assign users if they have no group-based policy assignment already. By default, the first policy in the list is chosen.</p>
User policy assignment	<p>Specify whether you want the user policy assignment to be fixed after the first synchronization, or if you want the service to check the group policy membership every time users are synchronized or group policy assignments are changed on the portal.</p> <p>Select “Follow group membership” if you want users’ policy assignments to change automatically when there are changes to their group membership. If you move someone to another group, he or she moves to a different policy. This is the default.</p> <p>Select “Fixed” if you want to manage policy assignments on the portal. When you select “Fixed,” the service makes a policy assessment for an individual user only when that user first appears in the system (in other words, is synchronized for the first time). It either assigns the user a group-based policy or the default policy specified above. If you want to move someone to a new policy, you need to do so on the portal.</p>
Email new users	<p>Select one of the radio buttons to indicate whether you want email sent to new end users to notify them that they are now protected by Websense blueSKY . You can send email to all new users, only those who do not have an NTLM identity, or no one.</p> <p>Be aware that sending to end users could flood your email servers with messages and slow down performance. You’re asked to confirm this decision. We recommend you do this at a quiet time.</p>
Email notification	<p>Choose which email you want to use to notify end users of their enrollment in Websense blueSKY . Initially, only the default message is offered, but you can create custom if desired. See Block and notification pages for more information.</p> <p>For sender’s address, enter the address from which you want notification messages sent to new users.</p>

6. Click **Submit** when done.

**Note**

You can turn off directory synchronization any time and revert to managing all users, groups, and email addresses on the portal. If you plan to do this, please see [Turn off directory synchronization, page 39](#) for possible considerations.

Set up authentication

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

On the **Contacts** page, set up authentication for the client machine. We strongly recommend that the client have its own username and password to gain access to the cloud service. This keeps the synchronization process separate from your other administration tasks and enables you to establish longer password expiration policies.

Once you establish a contact for the client machine, you configure the client to pass these logon credentials when connecting to the service.

1. On the portal main menu bar, click **Account Settings**.
2. Click **Contacts**.
3. In the Contacts section, click **Add**.
4. Enter identifying information for the client machine in the **First name** and **Surname** fields. For example, “Directory Sync” and “Client.”
5. Click **Submit**.
6. In the User Name field, click [here](#) to add a user name.
7. Enter a password for the client machine. It must conform to the password policy on the main Contacts page.
8. Enter a password expiration date for the client. To avoid having to regularly update it, this should be different than the regular account settings; it should span a longer period.
9. Under **Account Permissions**, check the **Directory Synchronization** box, and any other permissions you want to give this “user”. You can act as an administrator from this logon.
10. Click **Submit**.

Client tasks

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

The Directory Synchronization Client is designed to run on a machine with at least 2GB of RAM, and requires approximately 10MB of disk storage. The following operating systems are supported:

- ◆ Windows XP Professional Service Pack 2
- ◆ Windows Server 2003
- ◆ Windows Vista
- ◆ Windows 7
- ◆ Windows Server 2008

To download the client:

1. From the client machine, log on to the portal.
2. Select **Account Settings > Directory Synchronization**.
3. Under Download Directory Sync Client, download the directory synchronization client.
Select a client tool to download it. If you already have a Java Runtime Environment (JRE), download the tool without a JRE. Otherwise, download the one that includes a JRE. A JRE is required to run the client software.
4. When the download is complete, run the executable file.
5. Navigate through the installation wizard as prompted, accepting the license agreement and indicating where to install the application. Review the installation instructions in the client administrator's guide for assistance.
6. Configure the client as described in the client administrator's guide. Provide the logon credentials that you established as part of the configuration.

Maintenance

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

After directory synchronization is set up and running properly, you can perform the following tasks on the portal:

1. [View and manage user data](#). Note you cannot edit data that has been synchronized from your directory.
2. [Assign a group to a different policy](#)
3. [View and print reports](#)
4. [View recent synchronizations](#)
5. [Restore directories](#) to previous version
6. [Troubleshoot synchronization failures](#)
7. [Turn off directory synchronization](#)

View and manage user data

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

You can view account- or policy-level data about end users at any time. The portal provides a clear indication of which records are maintained in the service and which have been synchronized from your directory.

1. To view account-level data on users, select **Account Settings > End Users**.
2. Check the boxes on the left to indicate which search criteria to use.

3. Narrow down the search by entering or selecting precise data in the middle column.
4. Check the boxes on the right to indicate what information to include in the results.
5. Choose how many results to show per page and click **Search**.
6. From the resulting data, you can make individual edits or bulk edits. For example, you can:
 - a. Move user(s) to another Web policy, performing a manual override
 - b. Undo the manual override
 - c. Enable or disable Web access for user(s)
 - d. Delete user(s)

All changes made on this screen override any group/policy assignments (existing or future ones). To return to the automatic settings, manually undo your changes here.

You can view and manage user data at the policy level as well as using the End Users screen for the policy.

Assign a group to a different policy

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

You can modify the Web policy to which members (i.e., users) of synchronized groups are to be assigned. This assignment takes place either when the user is initially created on the cloud-based service or when group membership or group policy assignment changes, depending on how you configured the **User policy assignment** setting on the Manage Directory Synchronization page (see [Configure directory synchronization](#), page 30).



Note

Data from LDAP is read-only; you cannot change users and groups relationships that were synchronized from the client directory. If a change is required, you must make it in the client directory itself.

1. Open the policy to which you want to assign groups. For example, select **Web Security > Policy Management > Policies > DEFAULT**.
2. Click the **End Users** tab.
3. Under Directory Synchronization, click **Modify list of groups**.
4. Select the groups you want assigned to this policy.
5. Click **Submit**.

If you set **User policy assignment** to **Follow group membership** when you configured directory synchronization, the effect of this action is to assign all members of the group already in the service to this policy. Users that are not members of groups, or users in groups that are not explicitly assigned to a policy, are automatically

assigned to the default policy. All future additional users who are members of the group are synchronized into the policy as well.

If you set **User policy assignment** to **Fixed**, the change affects only future additional users.

View and print reports

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

You can view and print reports on the portal that show the history of synchronizations, including high-level statistics on success/failure and numbers of items synchronized.

The following reports are available:

Report	Description
Synchronization History Log	The history log provides a connection history for the specified period, up to 1000 rows.
Synchronization Time Summary	The time summary provides a list of the 20 longest synchronization times.

Click **Home > Reports > Services** to access them. See [Reporting](#) for more information.

View recent synchronizations

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

1. Select **Account Settings > Directory Synchronization**.

The Recent Synchronizations section shows your recent synchronization history.

Column Heading	Description
Date	The date and time that the synchronization was performed in coordinated universal time (UTC). Format YYYY-MM-DD HH:MM:SS.
Status	An indication of whether the synchronization completed or failed. Possible HTTP response codes include: <ul style="list-style-type: none"> • 200 OK - Completed successfully. • >400 - Synchronization failed <ul style="list-style-type: none"> • 403 Error text - The client synchronization failed for reasons given in the error text. For example: <ul style="list-style-type: none"> • 403 Groups contain circular references • 403 Transaction failed • 403 Attempt to overwrite portal managed group. • 403 Email address exists in another account • 503 Service Unavailable.
Type	The type of record that was synchronized: Users, Groups, Addresses, or Test. Test indicates that the client connected to the portal to verify its settings, but did not synchronize.
Additions	The number of new records added during the synchronization. If the synchronization is not yet complete, "In progress" is displayed.
Deletions	The number of records deleted during the synchronization.

2. Click the timestamp in the date column to view details about a specific synchronization.

In the resulting screen, you can see the time that the connection started and ended in the local time zone of the client machine. (This lets you see how long the synchronization took). You can view the IP address of the source connection, the username of the client initiating the synchronization, and the number of records amended, added, or deleted. You can also see reporting and logging information.

Restore directories

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

If necessary, you can undo the last directory synchronization and restore the system to its state before the synchronization.



Important

It is not possible to undo the restore, so changes you made on the portal between the last synchronization and the restore operation may be lost. You are warned of the potential impact and asked to confirm the action.

1. Select **Account Settings > Directory Synchronization**.
2. Click **Restore**.
3. Click **Restore** to restore your directory to the current backup version or click **Cancel** to cancel.
4. Confirm your action when prompted, “Are you sure?”

Troubleshoot synchronization failures

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Should a synchronization fail to complete, a record is saved by Websense blueSKY along with your details, date/time stamps, and an error message. You can access this information by selecting **Account Settings > Directory Synchronization**. See [View recent synchronizations, page 36](#) for more information. You can also view it in the Synchronization History log, available under **Home > Reports > Services**.

In the status column, any response code greater than 400 indicates a failed synchronization.

HTTP Response Code	Explanation	Recommended Action
403 Groups contain circular references	An attempt has been made to synchronize a hierarchy of groups that contain one or more circular references. For example, GroupA is a member of GroupB, but GroupB is a member of GroupA.	The list of groups forming the cycle are listed in the response code. Check these groups and fix the memberships to break the cycle.
403 Transaction failed	Further explanation is added to the response code to explain the problem. This is usually due to some uniqueness constraint failing--for example, if 2 users have the same email address or LDAP domain name.	Resolve the issue detailed in the full response code.
403 Attempt to overwrite portal managed group.	An attempt has been made to synchronize a group with the same name as a portal-managed group, and the Overwrite Portal Groups option is off.	On the Configure Directory Synchronization screen, check the Overwrite Groups box to allow overwriting, or rename the duplicate groups to remove the conflict.
403 Email address exists in another account	An email address in the LDAP directory already exists in another account.	Remove this email user from your directory if it is your error. If it is a valid address that you own, contact Customer Services to have the address removed from the other account.

HTTP Response Code	Explanation	Recommended Action
503 Service unavailable.	<ul style="list-style-type: none"> • The portal is heavily loaded, so a synchronization is not currently possible. • Synchronization is not enabled on the account • Your account has exceeded its daily synchronization limit 	<ul style="list-style-type: none"> • No action. The client automatically re-tries later. • Enable synchronization by selecting Account Settings > Directory Synchronization > Edit > Enabled. • Retry tomorrow (or when next scheduled).

Partially transmitted and temporarily stored data remains on the Websense blueSKY service for a few days as a possible debugging aid. This data is not used when you try to synchronize again.

Turn off directory synchronization

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

You can turn off directory synchronization any time and revert to managing all users, groups, and email addresses on the portal. To do so:

1. Cancel any scheduled synchronizations on the client machine. For more information, see the section “Removing the synchronization schedule” in the [Directory Synchronization Client Administrator’s Guide](#).
2. Log on to the portal.
3. Choose **Account Settings > Directory Synchronization > Edit**.
4. Clear the **Enable directory synchronization** check box.
5. Click **Submit**.



Important

Ensure that a synchronization is not under way when you disable directory synchronization. If a synchronization is running, you may end up with an incomplete set of data: for example, your groups might have synchronized successfully, but your users might not.

When you turn off directory synchronization, Group and user IDs on previously synchronized items are retained, so you can easily re-enable synchronization at a later date.

Please note that changes made manually on the portal to data items that were previously synchronized are lost if you later re-synchronize. When you re-enable synchronization, you are indicating that it is now the LDAP directory that holds the master data, and a full re-synchronization is performed.

4

Configuring Web Security

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Custom categories](#)
- ◆ [Protocols](#)
- ◆ [Block and notification pages](#)
- ◆ [Time periods](#)
- ◆ [Domains](#)
- ◆ [Full traffic logging](#)
- ◆ [Bypass settings](#)
- ◆ [Managing Network Devices](#)
- ◆ [Defining Web Policies](#)

Click **Web Security**, then **Settings** to configure web security for your account. You are presented with a number of tools and configuration options.

Custom categories

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Websense blueSKY categorizes websites into dozens of built-in categories to help you manage your end users' web surfing. See [Category list, page 92](#), for further information about the built-in categories.

You can also create your own custom categories, each of which comprises a set of sites (for example, "www.google.com") or URLs (for example, "http://www.yahoo.com/index.html"). Custom categories are created at the account level so that they are available to all policies.

Click **Web Security > Policy Management > Custom Categories** to view the categories for your account.



Note

The protocol and the port are always ignored, so both sites and URLs match HTTP or FTP requests on any port. Only sites match HTTPS requests, however. For an HTTPS URL, the browser does not send the full URL to the proxy.

If you have already created custom categories in a TRITON Web Security on-premises solution, you can import them to Websense blueSKY in CSV file format.

To create custom categories in the cloud service:

1. Click **Add**.
2. Assign a name to your new custom category and give it a description.
3. Click **Submit**.
4. Add s, URLs, or IP address ranges to the category. Format the IP address ranges in one of these ways:

Explicit address: a single address. Example: 216.27.61.137

Explicit range: 2 addresses separated by a dash (-). Example: 216.27.61.137-216.27.61.255

Subnet: An address followed by a slash (/) and the number of bits, which is a number between 1 and 32. Example: 216.27.61.137/24

Subnet with subnet mask: An address followed by a slash (/) and a netmask. Example: 216.27.61.137/255.255.255.0

Use IPv4 addresses only. Note that a space before and after the - and / is allowed.

IP address ranges are used to match IP addresses appearing in the host part of the URL.

5. Click **Add** again.

To import a custom categories file from TRITON Web Security:

1. Click **Print Policies to File** on the Web Security Policies page.
2. Locate the Custom Categories and Recategorized URLs sections in the output file.
3. Copy your custom categories and recategorized URLs to a CSV file using this format:

CategoryName, RecategorizedURL

CategoryName, RecategorizedURL

CategoryName, RecategorizedURL

4. Save the CSV file.
5. In the cloud service portal, click **Import File** on the **Policy Management > Custom Categories** page.
6. In the Import Custom Categories dialog box, browse to your CSV file and click **Import File**.

These custom categories can be used in the same way as the built-in categories; see [Category list](#), page 92, for further information.

Protocols

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

The **Policy Management > Protocols** page enables you to manage non-HTTP Internet traffic. Websense provides protocol groups in a master database that include similar types of Internet protocols (like FTP or IRC) and applications (like MSN Messenger or BitTorrent). The database of protocol groups is updated regularly. These protocols cannot be edited or deleted.

You can also add, edit, or delete custom protocols on the **Policy Management > Protocols** page. Custom protocols are available to all policies.

Use the **Search** field to search for a particular protocol or group in the protocols list. To delete a custom protocol, select it in the protocols list and click **Delete**.

Adding a custom protocol

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Use the following steps to define a custom protocol:

1. Click **Add** to open the Add Protocol page.
2. Enter a unique protocol name using only alphanumeric characters.
3. Select a group from the drop-down list (default value is **User-defined**).
4. Click **Add** to display the Add Protocol Identifier dialog box.
5. Specify the following identifiers for the custom protocol:
 - a. **Ports**: You can select **All ports** or **Specific port/range** (default selection) to indicate a single port or port range. Separate the components of a port range with a hyphen.
 - b. **IP addresses**: You can select **All IP addresses** or **Specific IP address/range** (default selection) to indicate a single IP address or address range. Separate the components of an address range with a hyphen.
 - c. **Transport method**: Select either **TCP** or **UDP**.

Transmission control protocol (TCP) is slower than UDP but provides reliable, ordered data delivery. User datagram protocol (UDP) is stateless and therefore faster than TCP, but it can be unreliable.
 - d. Click **OK**. Your identifiers appear in the Protocol Identifier list.
6. Click **Save**.

Edit protocol identifiers by clicking the Port/Range link in the Protocol Identifier list. In the Edit Protocol Identifier dialog box, modify your identifier values.

You can delete a set of protocol identifiers by selecting it in the Protocol Identifier list and clicking **Delete**.

Editing a custom protocol

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Edit a custom protocol by selecting it in the protocols list and clicking **Edit**. The Edit Protocol page appears with protocol information populating the fields.

Modify your identifier values by clicking the **Port/Range** link in the Protocol Identifier list and changing their values as needed in the Edit Protocol Identifier dialog box.

Block and notification pages

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Editing notification pages](#)
- ◆ [Language support](#)

Click **Web Security > Policy Management > Block & Notification Pages** to view or edit block page text and notification messages for your account.

When a Websense blueSKY policy denies access to a resource or needs to inform the user of an event, it can serve any configured notification page. There is a standard set of pages included with Websense blueSKY, and you can either modify these to suit your needs, or add your own pages. You can then refer to the notification pages from any of your policies.

The pages are grouped for ease of navigation. Click a down arrow next to a group name to see a list of all the pages within that group. To see all available pages, click **All**.



Note

Pages that you create are listed under Custom. To delete a custom page, click the delete icon next to the page name. The delete icon is displayed only if the custom page is not used in any policies.

Click the name of a page to edit its contents.

To create a new notification page:

1. Click **New Page**.
2. Enter a **Name** for the new page.

3. Enter a short **Description** of the page. This appears under the page name in the Block & Notification Pages list, and should clearly identify the purpose of the page to any administrator.
4. Click **Save**.

The Page Details page is displayed, with the name and description at the top. You can now edit the page as required.

For information about editing the content of a new or existing notification page, see [Editing notification pages, page 47](#).

Default notification page settings

Use the Settings area to configure default options for your block and notification pages. You can override any of these settings for individual pages.

Default language

The default language for block and notification pages is English. You can change this by selecting a different language from the **Default language** drop-down list .

If you select a different default language and then click **Save**, your changes are immediately visible to end users. Ensure that you have saved pages in the new default language; if a page is not available in the new default language, the English page is displayed.



Note

The end user registration pages for secure form-based authentication are already available in the following languages: French, German, Italian, Dutch, Spanish, Simplified Chinese, and Japanese.

See [Language support, page 50](#).

Default logo

By default, the logo displayed on the notification pages is the Websense blueSKY company logo. To change the logo:

1. Click **Edit**. The Default Logo popup window is displayed.
2. Select **Custom images**, and enter the URL of the image you want.
The image must be a JPEG, GIF, or PNG file. Click **Verify Image** to confirm the format and location of the image file.
3. Click **OK**. The new logo is displayed in the Settings area.

4. Click **Save**.



Note

If you choose to display a custom logo, we recommend that you host it on an HTTPS site. This ensures that your end users do not see warnings about unsecure elements on notification pages that use HTTPS, such as end-user registration and secure form authentication.

Default footer text

Any footer text that you specify appears at the bottom of each notification page. You may wish to use this area to provide contact information for end users.

To change the footer text:

1. Click **Edit**. The Footer Properties popup window is displayed.
2. Enter or edit text as required.
You can select all or part of your text and use the text formatting buttons to add bold, italic, color and other formatting. Hover over each text formatting button to see its function.
3. Click **OK** when done. The new footer text is displayed in the Settings area.
4. Click **Save**.

HTTPS notifications

To enable the cloud proxy to serve the correct notification page to the user for HTTPS sites – for example, a block page if the site is in a category that the end user is prevented from accessing, or the *Pre-logout welcome page* for authentication – you need a root certificate on each client machine that acts as a Certificate Authority for secure requests to the cloud proxy.

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

1. In the Settings area, 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 **Use Websense certificate to serve notifications for HTTPS pages**.
3. Click **Save**.

Editing notification pages

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Notification page variables](#)
- ◆ [Language support](#)

Each notification is a complete HTML page . The Page Details page presents a simple view of the page with editable sections, enabling you to customize the text and images.

To change the content of a notification page:

1. For custom pages, click **Edit** to update the page **Name** or **Description**. Click **Save** when done.
 2. To change the page name that appears in the browser's title bar, edit the **Page title** field.
 3. Hover your mouse over the page content to highlight the sections that are editable. To edit a line of text or block of content, click its section to open a text editor window.
 4. Edit the text as required.
 - You can select all or part of the text and use the text formatting buttons to add bold, italic, color and other formatting. Hover over each text formatting button to see its function.
 - To add a variable to the section, click **Variables/tokens**, and select from the drop-down list. See [Notification page variables, page 48](#).
- Click **OK** when done.
5. To edit the page footer:
 - a. Click the footer section to open a text editor window.
 - b. If you have already specified [Default footer text](#), clear the **Use default footer text** box.
 - c. Enter the footer text to use for this notification page. You can select all or part of the text and use the text formatting buttons to add bold, italic, color and other formatting.
 - d. Click **OK** when done.
 6. To edit an image on the page:
 - a. Click on the image. The Image Properties popup window is displayed.
 - b. To use one of the standard images provided by Websense blueSKY, select **Standard images** and click on the image you want.
 - c. To use an image of your choosing, select **Custom images** and enter the URL of the image you want.

The image must be a JPEG, GIF, or PNG file. Click **Verify Image** to confirm the format and location of the image file.

- d. Click **OK**.
7. To view and edit the HTML source, click **HTML Editing**. Any valid HTML may be used within a notification page.



Note

If you edit a page in the HTML view and then click **Basic Editing** to return to the basic editor, you will lose any changes made in the HTML view.

8. To see how the page appears to end users, click **Preview**. The page appears in a separate window.



Note

Your browser may warn you that you are switching to an unsecured connection.

9. Click **Save** when done.

If you wish to discard customizations to a standard page, click **Revert to Default**. This removes all changes that have been made to the page in your account, and reverts the page to the original one supplied in Websense blueSKY.

Notification page variables

Some mark-up strings or variables are available. At the time a page is rendered to the end user, these are replaced either with request-specific or user-specific data or with values configured elsewhere in the system. The parameters are generally textual components of the page and their use should be clear from the page preview.

Variables have the following attributes:

- ◆ Variables are always surrounded by underscores, for example, `_URL_`
- ◆ If Websense blueSKY recognizes a variable, it replaces it with the value it represents. If it does not recognize a variable, it leaves it untouched.

The following variables are available in Websense blueSKY. Note that when you edit a page, the **Variables/tokens** drop-down list contains only the variables that are relevant to that page.

Variable	Description
Category	The web category that applies to the requested site and has triggered the block or notification page.
Client IP address	The IP address of the user attempting to authenticate, register, or access a web page. This is optional on most pages, and can be submitted for reporting purposes when a user authenticates or confirms that they want to access the URL via quota time or continue/confirm. It is mandatory on the secure form logon page.
Agree Acceptable Use Policy	Link to accept your Acceptable Use Policy and continue to the requested website. Mandatory on the Acceptable Use Policy page.
Close Acceptable Use Policy page	Link to close the Acceptable Use Policy page without agreeing to the policy. Mandatory on that page.
Custom text	Use to include your own text on the Acceptable Use Policy page.
File extension	Displays the file extension that the user has attempted to access when file extension blocking is in use.
Maximum file size	Displays the maximum file size allowed when file size blocking is in use.
Requested file size	Displays the size of the file that the user has attempted to access when file size blocking is in use.
Host name	The host name of the site that the user is trying to access.
Login host name	The host name used for transactions involved in logging on to the cloud service. For example, clicking the 'Log in' button on the Welcome page submits a form to this host.
Login URL	Link to log on to the cloud service using basic authentication or NTLM identification.
HTTP request method	The 'method' in the HTTP request that is being handled (for example, 'GET', 'POST')
NTLM domain name	The domain part of a user's NTLM ID.
NTLM ID	User's NTLM ID, in the format domain\username.
NTLM username	The user name part of a user's NTLM ID.
Policy name	The Websense blueSKY policy that has been applied to the web request.
Protocol	Either HTTP or HTTPS. Used in embedded URLs, such as image links, so the service can use a common page for mixed HTTP and HTTPS without getting browser warnings that the page uses one protocol but image links use the other one.

Variable	Description
Quota time disabled	Used on the quota page to disable the OK button when the user's daily quota has been used up.
Quota remaining	The number of minutes remaining in the user's daily quota time.
Quota session length	The session length available to the user if they choose to use quota time to browse the site they have requested, as well as other sites in that category (if per-category quotas are enabled) or that are in categories set to use quota time.
Reason	The reason the request was blocked. Only valid on pages triggered by a blocked request.
Registered email address	End user's email address as registered in the cloud service. This address is used to send emails as part of the end-user registration process and the password reset process.
Registration URL	Link included in forgotten password and end-user registration email notification templates. When clicked, the link takes the user to a page where they can reset their password or complete their registration. This is mandatory in both email notifications.
Requested URL	The URL that the user is attempting to access, and that has caused the block or notification page to be displayed. If the notification page is a request for authentication, or to use quota time or continue/confirm, the user is automatically redirected to the URL when they authenticate or confirm.
Username	End user's user name. Can be used on the Acceptable Use Policy compliance page, or in end-user notification emails for password resets and self-registration.

Language support

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Block and notification pages can be displayed to end users in any language you require. If you create multiple language versions of standard or custom pages, the most appropriate language is served to end users based on their browser settings, allowing a single corporate policy to be applied to a multi-national user base.

The default language for block and notification pages is English. You can change this by selecting a different language from the **Default language** drop-down list in [Default notification page settings](#).

To add a different language version to a notification page:

1. Click on the page name to open it for editing.
2. Click **Add Language**.
3. Select the language(s) you wish to add from the Available languages list. You can use the Shift and Ctrl keys to select multiple languages.
4. Click the > arrow to move the languages to the Selected languages list.

5. Click **OK**.

The language(s) you selected is now available in the **Languages** drop-down list. Select a language from the list to edit the page content for that language, as described in [Editing notification pages, page 47](#).

To delete a language version of a notification page, click **Delete Language**.

Time periods

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Websense blueSKY allows you to configure policies that restrict web surfing by time of day for either the whole policy or for categories, users, and groups. When an exception rule is configured, it is applied to a time period.

Click **Web Security > Policy Management > Time periods** to configure time periods for your account. These are configured at the account level so that they can be available for use in multiple policies, if required.

Each account is provided with 4 default time periods.

To edit or view a time period

Click the name of a time period, for example “Working hours.”

You can assign the time zone for the period, which is typically the default for the policy or connection where the users are located (see [Proxied connections, page 74](#)).

The dark area defines the actual time period. Each division is a 15 minute period and can be set with either a single click or by clicking and dragging to produce a wider area. As you roll your mouse over the area, the absolute time is displayed below the time chart.

To define a new period

1. Click **Add time period**.
2. Enter a name and description for the new period.
3. Choose a time zone.

If you do not want to use the default for the policy or connection, you can select a particular geographical location and city (for example Australia/Sydney), or a time zone such as GMT or UTC.



Note

Daylight saving time is supported where valid on all time zones except GMT and UTC, which are static. For example, if you select GMT, British Summer Time is not taken into account for this time period.

4. Click the **Paint** radio button.
5. Click and drag the mouse over the desired time period. Release the mouse when you're done.
6. Click **Submit** to save your changes.

To delete a period

If you want to delete a time period, make sure that it is not being used by any rules first. If it is in use, the **Delete** button is greyed out.

Domains

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Policy-level domains](#)
- ◆ [Account-level domains](#)
- ◆ [Editing a domain](#)
- ◆ [Permissions implications](#)
- ◆ [Legal requirements](#)

Websense blueSKY uses the concept of end-user self-registration as an enabler for user authentication. For self-registration, a user has to exist within an email domain that can be configured at either the account or policy level.

Before reading this section, we recommend that you read [Time periods, page 51](#) and [Proxied connections, page 74](#).

Policy-level domains

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Domains](#)
- ◆ [Account-level domains](#)
- ◆ [Editing a domain](#)
- ◆ [Permissions implications](#)
- ◆ [Legal requirements](#)

Policy-level domains are created in the policies themselves. To create a policy-level domain:

1. Select **Web Security > Policy Management > Policies**.
2. Click the name of the policy to open.
3. Click the **End Users** tab.
4. Under Self Registration, click **Add**.

No policy-level domain can exist in multiple policies or accounts.

When you are adding a policy-level domain, some options are greyed out, because they are only applicable to account-level domains.

Users with an email address in this domain are registered to the policy to which the domain is assigned.

Account-level domains

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Domains](#)
- ◆ [Policy-level domains](#)
- ◆ [Editing a domain](#)
- ◆ [Permissions implications](#)
- ◆ [Legal requirements](#)

You can use account-level domains to register those with a policy in an account. The actual policy they register with is determined by the IP address from which they register (see [Proxied connections, page 74](#), for an explanation). Account-level domains must have a default policy for remote users. If there is no default policy, then remote users cannot register and receive an error message when they try to do so.



Note

If all users are on a single email domain and you intend having multiple policies, you must configure account-level domains and assign to all policies.

Click **Web Security > Settings > Domains** to see the end-user registration domains, and the policy each domain is associated with. If they are account-level domains, the words “By connection” are shown instead of a policy name.

Editing a domain

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Domains](#)
- ◆ [Policy-level domains](#)
- ◆ [Account-level domains](#)
- ◆ [Permissions implications](#)
- ◆ [Legal requirements](#)

In the list of domains, click the name of a domain you want to edit, and then click **Edit**.

A domain can be associated with a specific policy or all policies. If you select **Associate this domain with all policies**, you are prompted to assign a default policy for remote users. If no account-level domains are assigned, remote users are registered into the policy associated with the account to which their domain is assigned.

If remote users try to register using an email address that is associated with an account-level domain and there is no default policy, they receive an error message.

Permissions implications

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Domains](#)
- ◆ [Policy-level domains](#)
- ◆ [Account-level domains](#)
- ◆ [Editing a domain](#)
- ◆ [Legal requirements](#)

Administrators who have permissions only for individual policies can access domain configuration only from within the policy, and they cannot amend account-level domains. They also receive a restricted set of controls when editing policy-level domains. From this view, they can see all domains but have editing rights only to the policy-level domains associated with their policy.

Legal requirements

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Domains](#)
- ◆ [Policy-level domains](#)
- ◆ [Account-level domains](#)
- ◆ [Editing a domain](#)
- ◆ [Permissions implications](#)

Your terms and conditions for use of the service include a clause that restricts the use of domains to those that are legally registered to your organization. [Bulk registering end users, page 81](#), explains the process of bulk registration, where the Websense blueSKY service sends email to a list of email addresses uploaded to the service. The legal restriction is to prevent someone from maliciously or unintentionally spamming a third party with email originating from Websense blueSKY.

Full traffic logging

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Full traffic logging enables you to download raw proxy request data from Websense blueSKY for retention and analysis.



Important

The full traffic logging feature is not available by default. To make it available in your account, contact Support.

Check the **Enable full Web traffic logging** box to enable log retention for your account. Note that if you enable this feature, Websense blueSKY starts saving large amounts of data that you must download to your own systems.

Log data is retained for 14 days. If you do not download the traffic data for a period of 14 days, log retention is disabled for your account.

For full details of how to set up and use full traffic logging, we strongly recommend you read the “Configuring Full Traffic Logging” technical paper.

You can also retain full traffic logs for specific policies. For more information, see [General tab, page 70](#).

Bypass settings

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Bypassing authentication settings](#)
- ◆ [Bypassing certificate verification](#)

Websense blueSKY includes the following options for bypassing security and authentication checks, if required for your end users:

- ◆ Authentication bypass enables you to add custom settings for Internet applications and websites that cannot authenticate with the cloud service. See [Bypassing authentication settings](#), page 56.
- ◆ Certificate verification bypass enables you to specify trusted HTTPS domains that your end users can always access even if the certificate is detected to be invalid. See [Bypassing certificate verification](#), page 58.

Bypassing authentication settings

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Bypassing certificate verification](#)

When Websense blueSKY is enabled, occasionally some Internet applications and websites cannot authenticate with the cloud-based service. This might occur with, for example, instant messaging programs, antivirus updates, or software update services.

If you are experiencing problems with Internet applications, the **Web Security > Settings > Bypass Settings** page enables you to add and edit custom settings to change the default Websense blueSKY behavior for failing applications or sites.

To allow particular applications that do not properly handle authentication challenges to bypass authentication, you can specify user agents, domains, URLs or a combination of these options.

A user agent is a string sent from your browser or Internet application to the server hosting the site that you are visiting. This string indicates which browser or application you are using, its version number, and details about your system, such as the operating system and version. The destination server then uses this information to provide content suitable for your specific browser or application.

For example, this is a user agent for Firefox:

Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.6)

In this example, Windows NT 5.1 indicates that the operating system is Windows XP, and the language it uses is US English.

To get the user agent string for your browser, enter the following in the browser's address bar:

```
javascript:alert(navigator.userAgent)
```

To add a setting for an application or site:

1. Click **Add** under **Authentication Bypass**.
2. Enter a **Setting Name**. This name appears in the Authentication Bypass list on the Bypass Settings page, and you can click on it at a later date to edit your settings.
3. Define the user agents, if any, for the rule:
 - If the application does not send a user agent string to the Internet, select **No user agent header sent**.



Note

This option will match against all applications that do not send a user agent. In this case, we recommend you refine the rule by entering one or more URLs or domains in the **Apply to Destinations** field.

- If you want to apply the custom authentication to one or more user agents, select **Apply custom settings for the following user agents**. To specify particular user agents, enter each user agent on a separate line. Use the asterisk wildcard to match one line to multiple user agent strings, for example Mozilla/5.0*.
 Leave the field blank to match against all user agent strings. You might want to do this if you are setting up a custom rule that applies to all browsers on all operating systems in your organization.

4. Define the URLs or domains (if any) for the rule in the **Apply to Destinations** field, by entering each URL or domain on a separate line.

URLs must include the protocol portion (http://) at the beginning and a forward slash (/) at the end – for example, http://www.google.com/. If these elements are not present, the string is treated as a domain. Domains cannot include a forward slash at the end – for example, mydomain.com.

Use the asterisk wildcard to match one line to multiple destinations: for example, entering *.mydomain.com would match against all domains ending in 'mydomain.com.'

Leave the field blank to match against all domains and URLs. You might want to do this if you are setting up a custom rule that applies to a specific user agent that accesses multiple sites.

5. Select the authentication capability for the custom rule.
 - **Use defaults:** Uses your default authentication method.

- **NTLM:** Uses NTLM identification for the specified user agent(s) and destination(s). If an application is not NTLM-capable, basic authentication will be used instead. For more information about NTLM identification, see [NTLM transparent identification, page 84](#).



Note

You must have NTLM identification enabled for your account to use this option.

- **Form login:** Displays the secure login form to users before they use their Websense blueSKY credentials to proceed over a secure connection. For more information, see [Access Control tab, page 75](#).
 - **Basic:** Uses the basic authentication mechanism supported by many web browsers. No welcome page is displayed. For more information on basic authentication in Websense blueSKY, see [Access Control tab, page 75](#).
 - **No authentication:** Bypasses all authentication and identification methods in Websense blueSKY. Select this option for Internet applications that are incapable of authentication.
6. Optionally, you can bypass all filtering for the specified user agent(s) and destination(s) by selecting **Bypass content analysis**.



Important

We strongly recommend you select this option only for applications and sites that for some reason do not work well with Websense blueSKY and that you trust implicitly. Selecting this option could allow viruses and other malware into your network.

7. Click **Submit**.

To view the user agents that have made authentication requests via the cloud-based service, run the User Agents by Volume report (click the link on the Bypass Settings page, or navigate to **Web Security > Reports > Volumes**).* If a user agent in this report has a high number of authentication requests, it may be experiencing authentication problems. You can click on a user agent in the report to add a new custom authentication rule.

Bypassing certificate verification

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Websense blueSKY verifies certificates for HTTPS sites that it has decrypted and analyzed. Certificate verification is enabled by default on the Bypass Settings page, and happens automatically in one of the following cases:

- ◆ SSL decryption has been enabled for web categories (see [SSL Decryption tab](#), page 104).
- ◆ You are using secure form-based authentication (see [Access Control tab](#), page 75).

Certificate verification checks are numerous and apply to all certificates in the trust chain. For example:

- ◆ The certificate must be issued by a trusted Certificate Authority (CA).
- ◆ The certificate must be current (within its “Valid from...to...” date range).
- ◆ The certificate must not be on a revocation list (either CRL or OCSP).

To choose whether or not to use certificate verification, in the Certificate Verification Bypass section, set **Perform certificate verification** to On or Off.



Important

We strongly recommend that you verify certificates for HTTPS sites. If you switch this option off, there is a chance of increased security risks from malicious sites with certificates that misrepresent their identity (for example, a site called google.com pretending to be Google).

If certificate verification fails, the end user sees an error page and cannot access the website unless you allow them to access sites with certificate errors by marking **Allow end users to bypass all certificate errors**. In this case, end users see a notification page informing them that a certificate error has been detected, and have the option to either proceed to the site or go back.

If you choose to perform certificate verification, you can maintain a list of domains and IP addresses for which Websense blueSKY bypasses certificate verification errors. This enables end users to visit a site even if the certificate is invalid. You may want to do this for sites that you trust even if, for example, the certificate has expired, is not yet valid, or is self-signed.

You can manage domains and IP addresses for bypass as follows:

- ◆ To add items for certificate verification bypass, enter one or more domain names or IP addresses separated by commas, then click **Add**. IP addresses can also include the port number, for example 127.0.0.1:80. You cannot add IP address ranges.
- ◆ To delete a domain name or IP address from the bypass list, select the item and click **Delete**. You can use the **Ctrl** and/or **Shift** keys to select multiple items for deletion.

Click **Save** when done.

5

Managing Network Devices

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Configuring Web Security](#)
- ◆ [Defining Web Policies](#)

Click **Network Devices** in the toolbar to display the Network Devices page, where you can add and control all the appliances in your network.

Managing Websense IQ-Series Appliances

The IQ-Series Appliances list appears at the top of the Network Devices page. Columns contain the following information for each appliance shown:

Item	Description
Name	Appliance name, specified when an appliance is added in the cloud service. Click the name link to open a dialog box in which you can edit appliance settings.
Enabled	Indicates whether the appliance is enabled in the cloud service.
Description	Appliance description, specified when an appliance is added in the cloud service.
Host name/FQDN	Appliance host name or FQDN, specified on the appliance. If the appliance is not registered, or this information has not been received from the appliance, the display is "N/A".
Version	IQ-Series appliance version. If the appliance is not registered, or this information has not been received from the appliance, the display is "N/A".
Connectivity	Indicates connectivity status for the appliance (OK, Not registered, or Error). Hover your mouse over the status link to display details about the appliance and its connectivity status.

Item	Description
Alerts (last 24 hours)	<p>Displays the number of alerts for the appliance for the past 24 hours, along with an icon indicating the highest severity level represented among the alerts. If the appliance is not registered, or it has not generated alerts for the past 24 hours, this column displays “No Alerts”.</p> <p>Click the alert number to view a complete list of alerts for the appliance. See Viewing alerts, page 67.</p>
Web Policy	<p>Displays a policy name if the appliance is assigned to a policy. An entry of “N/A” indicates that the appliance is assigned to a policy, but the cloud service does not recognize the policy name.</p>
Last Response	<p>Shows the date and time of the latest response from the appliance.</p> <p>If the appliance is not registered, or has not sent any information to the cloud service, the display is “N/A”.</p>

The following activities can be performed from the Network Devices page:

- ◆ [Adding an appliance](#)
- ◆ [Registering an appliance](#)
- ◆ [Changing the appliance password](#)
- ◆ [Viewing appliance properties and statistics](#)
- ◆ [Deleting an appliance](#)

Adding an appliance

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Use the following steps to add an appliance to the cloud service:

1. Click **Add** below the appliances list.
2. 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 service, but allows all web traffic to pass through unfiltered.
 - d. Specify the web policy and associated time zone used to filter traffic from this appliance.
 - 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.
3. 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**.
 - 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.
 For information about tagging traffic explicitly generated by this device using the appliance user interface, see the topic “Routing” in the appliance Help.
 - 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.
4. In the Authentication tab:
- a. If you wish to use transparent NTLM authentication, 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. For more information, see the *Websense blueSKY Getting Started Guide*.

- 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.
5. 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. This must be in PEM format. 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.
The certificate chain should include the root CA, and optionally additional intermediate CAs.
- b. If you want to specify your certificates later, mark the **I want to define certificates later** option.



Important

It is recommended that you define certificates when you add an appliance, in order to avoid browser warnings regarding SSL termination block, authentication, or quota/confirm operations. Some browsers, for example later versions of Chrome, may block the transaction and display an error message.

Be sure to perform the following:

- ◆ Generate a CA certificate. Each appliance should have a valid X.509 identity certificate with an unencrypted key. This certificate can be generated using a variety of tools, for example OpenSSL. For details and an example, see [Generating a certificate](#) below.
- ◆ Import this certificate to all relevant browsers.
- ◆ Upload this certificate to each appliance using the Certificates tab.

To use the cloud service SSL decryption feature, you should also install the Websense root certificate on each client machine. See [Enabling SSL decryption, page 105](#).

6. Click **OK**.

Generating a certificate

Each appliance should have a valid X.509 version 3 identity certificate in PEM format with an unencrypted key. This 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.

Registering an appliance

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

After your appliance is configured and connected to your network, you must register the appliance with the cloud service:

1. If you have more than one appliance, ensure you select the radio button (to the left of the appliance list) of the appliance you want to register.
2. Click **Register** below the appliance list to open the Register Appliance box.
3. Copy the registration key that appears in the **Registration key** field.
4. Paste this key into the **Registration key** field that appears when you first log in to the appliance after completing the first-time configuration wizard.
5. Click **OK**.

Changing the appliance password

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

You can change the appliance password on the Appliances page. If you have more than one appliance, select an appliance in the list. Then click **Change Password** below the appliances list, and enter and confirm your new password in the Change Password dialog box. It may take several minutes for the new password to update on the appliance.

- ◆ The password must be between 8 and 30 characters.
- ◆ Strong passwords are recommended, including at least one uppercase letter, lowercase letter, number, and special character (such as hyphen, underscore, blank or other punctuation character).

- ◆ Non-Latin characters are not accepted.



Important

You must change the initial password on the appliance itself in order to register and manage the appliance.

Viewing appliance properties and statistics

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Select an appliance row in the appliances list and click the **Properties & Statistics** link below the list to open a box with 3 tabs:

- ◆ Properties
- ◆ Version History
- ◆ Statistics



Note

Status information sent to the cloud service from the appliance may take up to 15 minutes to be reflected in the cloud portal.

Properties

The **Properties** tab displays system information about the selected appliance, including name, description, host name or FQDN, version, platform, uptime, and the date/time of the latest appliance update. An indication of whether the appliance is enabled in the cloud service is also displayed.

Version History

Use the **Version History** tab to keep appliances up to date with the latest releases. You can check for and download product upgrades from this page. The current appliance version and date of installation appear at the top of the page.

The appliance checks with the cloud service for available upgrades every 6 hours. Downloading an upgrade makes it available to an appliance for installation at the next update from the cloud service.

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

The Action column contains an icon that, when clicked, downloads an available upgrade to an appliance.

The Upgrade History table provides a record of upgrade releases that have been applied to an appliance, including version number, upgrade date, and status

(successful or unsuccessful download and installation). The Action column contains an icon that opens the Release Notes for an installed upgrade.

Statistics

The **Statistics** tab displays graphical representations of the following system information for an appliance:

- ◆ Web transactions rate, showing transactions per second
- ◆ CPU usage, showing CPU availability levels
- ◆ Bandwidth, showing protocol and web traffic bandwidth usage levels
- ◆ Hard disk usage
- ◆ Memory usage
- ◆ Peaks for concurrent web requests and sessions

Select a graph from the Display drop-down list, and a time range (24 hours or 7 days) from the Time range drop-down list, and click **Go**.

Viewing alerts

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

In the appliances table Alerts column, click the alert number for an appliance to view a complete list of alerts for that appliance. The alerts page displays appliance alert events from the previous 24 hours, along with the date/time of alert occurrence. Change the Time range drop-down to see alert events for the last 7 days, The alerts are sorted by date, with the most recent alerts first.

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, because system operation is compromised

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

Deleting an appliance

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Delete an appliance from the appliances list by selecting the desired appliance row and clicking **Delete**.

6

Defining Web Policies

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Testing policy filtering](#)
- ◆ [Custom categories](#)
- ◆ [Block and notification pages](#)

On the **Web Security > Policy Management > Policies** page, there is a list of policies currently configured for your account. Click a policy name to view or edit a policy, or click **Add** to add a new policy.

There are several tabs associated with each policy. Depending on your subscription settings, you may not see all the tabs:

- ◆ [General tab](#)
- ◆ [Connections tab](#)
- ◆ [Access Control tab](#)
- ◆ [End Users tab](#)
- ◆ [Web Categories tab](#)
- ◆ [Protocols tab](#)
- ◆ [Application Control tab](#)
- ◆ [File Blocking tab](#)
- ◆ [Web Content & Security tab](#)
- ◆ [SSL Decryption tab](#)

Standard account-level settings are shown in [Standard Web Configuration](#), page 125.

Testing policy filtering

Use the Filtering Test section on the **Policies** page to check how a URL is filtered by your policies. You can also test particular situations that may be causing issues for your end users – for example including a user name, or user agent header.

To run a filtering test:

1. Under Filtering Test, enter the full URL that you want to test, including the http:// or https:// part.
2. Optionally, enter the email address of an end user registered or synchronized with your account.
3. Set the **Source IP** for the filtering test. By default this is the current IP address that you have used to access the cloud portal. Use **Other IP** to specify a different IP address that is registered as a proxied connection in one of your policies, or select **Unknown IP** if you are testing a roaming user scenario.



Note

If you select **Other IP** and then enter an IP address that is not associated with your account, an error message results.

4. If you wish to specify a particular user agent that may be causing filtering issues mark **Include user agent header** and enter the user agent string in the field provided.
5. Click **Test**.

The results popup window displays the following information:

- The details that you entered, including the user email address and user agent if defined
 - The policy filtering the URL, as derived from the source IP that you selected
 - The category or categories that the URL is in
 - The filtering action applied to the URL in this policy
6. Click **Close** when you are done.

General tab

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [*User and group exceptions for time-based access control*](#)

Use the General tab to configure settings that cover basic aspects of your users' web browsing, for example availability at certain times of the day, quota time limits, and agreement to your acceptable use policy.

If you make any changes to this tab, click **Save** when done.

Policy name

The name of the policy, which you may want to rename from Default to something more meaningful to your organization, especially if you have a requirement for multiple policies.

Administrator email

This is the email address for the web administrator of this policy. This email address is used as the address from which system messages are sent. Your users may occasionally reply to these messages, so this should be an email address that is monitored by your IT staff or administrative contact.

Policy template

Websense blueSKY includes several policy templates. Each template determines which web filter categories are blocked and which are permitted for a policy.

You can select a policy template only when creating a new policy. Once you have saved your settings for a new policy on the General tab, you cannot select a different template.

The following predefined policy templates are available for Websense blueSKY:

- ◆ **Default** blocks a default set of categories, including categories relating to adult material, drugs, violence, productivity, and security.
- ◆ **Basic** blocks the most frequently blocked categories and permits the rest.
- ◆ **Basic Security** blocks only categories considered to be a security risk.
- ◆ **Monitor Only** permits all categories.

Once you have selected a policy template for Websense blueSKY, go to the [Web Categories tab, page 87](#) to see the filtering actions applied to categories for that template. You can still refine your web filtering further by changing the actions for individual categories.

Time zone

To use time-based web filtering, Websense blueSKY must first determine the time zone where users are located. The time zone you set can be used as a single zone for the whole policy, or you can set up time zones for one or more of your proxied connections that override the time zone on the General tab (see [Proxied connections, page 74](#)).

Daylight saving time is supported where valid on all time zones except GMT and UTC, which are static.

Internet availability

Use this option to configure time-based web filtering in the policy. The default setting is to allow Internet access at all times, although you can apply user and group-based exceptions (see [User and group exceptions for time-based access control](#), page 73).

Alternatively, you can restrict all access by time and display an appropriate block page when access is unavailable. There are 2 formats for this:

1. Block access for the duration of a defined period (for example, during working hours).
2. Block access outside a defined period (for example, allowing users to access the Internet only during their lunch period).

The drop-down list contains the standard time periods and any custom periods you have set up (see [Time periods](#), page 51).

Full traffic logging



Important

The full traffic logging feature is not available by default. To make it available in your account, contact Support.

If you have the full traffic logging feature, by default all web policies have the logging setting that you define at the account level. If you want to override the default log retention for a particular policy, change the selection in the Full traffic logging drop-down list from **Use account default** to either **Enabled** or **Disabled**.

For full details of setting up and using full traffic logging, see the “Configuring Full Traffic Logging” technical paper.

Confirm timeout

Enter the maximum time in minutes (default 10) that a user who clicks Continue can access sites in categories governed by the Confirm action. See [Filtering actions](#), page 88.

Quota time

Use this option to configure quota times for web categories accessed by users in this policy. See [Using quota time to limit Internet access](#), page 90 for more information. Select one of the following:

- ◆ A **Daily quota** applies to all users accessing categories with Quota as the filtering action or exception. Enter the **daily limit** in minutes (default 60) for all users of this policy. Then define the **session length** in minutes (default 10) during which users can visit sites in quota-limited categories.

- ◆ A **Per-category quota** allows you to specify a **daily limit per category** and a **session length per category** that applies to all quota-limited categories by default. You can then change the daily quota time settings for particular categories or filtering exceptions on the Web Categories tab. See [Managing categories and filtering actions, page 87](#).

A session begins when the user clicks the Use Quota Time button.

The daily quota allocation for users within a policy is refreshed at midnight in the time zone defined for the user's proxied connection. If no specific time zones are defined in either the proxied connection or the policy, the quota allocation is refreshed at midnight UTC.

If you change the total quota time or session time after a user has started to use their daily quota or has received the quota block page from the cloud-based service, the changes will not take effect until the next day. Similarly, if you move a user to a different policy after they have started to use their daily quota or has received the quota block page from the cloud-based service, the change does not take effect until the next day.

Search filtering

Search filtering is a feature offered by some search engines that helps to limit the number of inappropriate search results displayed to users.

To activate this option, select **Enable search filtering**.

Ordinarily, Internet search engine results may include thumbnail images associated with sites matching the search criteria. If those thumbnails are associated with blocked sites, Websense blueSKY prevents users from accessing the full site, but does not prevent the search engine from displaying the image.

When you enable search filtering, Websense blueSKY activates a search engine feature that stops thumbnail images associated with blocked sites from being displayed in search results.

User and group exceptions for time-based access control

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Internet availability](#)

You can apply both user and group exceptions to any time-based access control that you set up. To view the list of exceptions, click the link next to **Internet availability**.

To edit an exception, click the exception, then click **Edit**.

To add an exception:

1. Click **Add exception**.
2. The rule **State** is set to ON by default, meaning the rule will be enabled for the users and groups you select. If you want to set up a rule but not enable it immediately, click the State switch to set it to OFF.
3. Enter a **Name** and **Description** for the rule.
4. Choose the notification page that appears to users in this exception.
5. Select the **Time period** during which the rule is active. If you select **During** or **Outside**, the drop-down list contains the standard time periods and any custom periods you have set up (see [Time periods](#), page 51).
6. For an exception that should be applicable to roaming users only, mark **Apply only when user is roaming**.
7. Do one of the following:
 - a. To set up an exception for specific users or groups, select **For these users and groups**. You can then enter a comma-separated list of email addresses, or select one or more groups, or both.
 - b. To set up an exception for everyone except those in a specific group, select **For everyone not in the group**, and choose a group from the drop-down list.
8. Click **Submit**.

Connections tab

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Proxied connections

Most organizations have at least 1 proxied connection. For Websense blueSKY, your proxied connection is a Websense IQ-Series appliance. An appliance may be assigned to only 1 policy.

Each proxied connection has a time zone setting. This is defined when you add a new appliance to your network.

If you have a single policy for multiple Internet gateways in different countries, you may want to set each to a different time zone. If all connections are in the same time zone, it is easier to set the time zone for the complete policy (see [Time zone](#), page 71) and leave the connection setting as 'use policy time zone'.

Daylight saving time is supported where valid on all time zones except GMT and UTC, which are static.

Applying a policy to requests

Browser requests arriving from the proxied connections are handled by Websense blueSKY according to the rules within this policy. See [Access Control tab](#), page 75 for further information about end-user authentication.

Non-proxied destinations

It is often desirable to avoid connecting via a proxy service for certain sites. For example, internal sites may not be accessible from the Internet, so the cloud service cannot serve them. In these cases, you should define non-proxied destinations. A non-proxied destination can be a domain name, an IP address, or an IP subnet.

Recommended non-proxied destinations include organizational webmail sites, internal IP addresses, and system traffic such as Microsoft and antivirus updates.

Click **Add** under Non-Proxied Destinations to add a new destination.



Note

Exceptions for protocols other than HTTP or HTTPS should be defined on a policy's Protocols tab.

Access Control tab

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [NTLM identification](#)

Use the Access Control tab to configure how your end users are identified by Websense blueSKY. You can configure multiple authentication or identification options for your users if required.

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, depending on your subscription settings, inappropriate content. However, most customers want to tailor the service to align it with their Internet acceptable use 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. This requires users to identify themselves to Websense blueSKY.

There are a number of events that can lead to an end user being asked to authenticate:

- ◆ The user is attempting to access a website for which there is a group or user exception. At this point, Websense blueSKY needs to find out who the user is in order to determine whether the exception applies.
- ◆ You have set up authentication options on the Access Control tab.

To configure user authentication:

1. Under **Authentication Settings**, define when to authenticate.

- Select **Always authenticate users on first access** to force all users of this policy (whose source IP address or appliance is configured on the Connections tab) to identify or authenticate themselves to proceed. If they do not, they are unable to use the cloud service.
2. Select the authentication methods you wish to use.

If you do not select any authentication methods, when users try to access a website, they are presented with a basic authentication dialogue into which they must enter their Websense blueSKY logon credentials to proceed.

 - Select **NTLM transparent identification** to identify users in this policy with their NTLM credentials. Then, select the NTLM registration page or use the default setting. See [NTLM identification, page 77](#), and [NTLM registration page, page 77](#).
 - Select **Secure form-based authentication** to display a logon form to the end user. When the user enters their Websense blueSKY credentials, they are sent over a secure connection for authentication.

If the users have not previously registered to use the service, they can do so by clicking **Register**. This takes them into the registration process. See [End Users tab, page 79](#) for further details.

Note that manual authentication is always used if neither of the above methods is available.
 3. Select **Welcome page** to show a configurable welcome page to end users prior to the basic authentication dialog box, if their browser supports it. See [Pre-logon welcome page, page 76](#).
 4. Click **Save**.

Pre-logon welcome page

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

When you select **Welcome page (where client software supports it)**, a configurable welcome page is presented to end users prior to the basic authentication dialog box, if their browser supports it. You can specify a single page that is presented for connection requests or different pages for requests using HTTP. The default pages provide three buttons: **Log in**, **Register**, and **Forgotten your password?**

- ◆ **Log in:** To continue, users click **Log in** and are presented with the basic authentication dialogue.
- ◆ **Register:** If the users have not previously registered to use the service, they can do so by clicking **Register**. This takes them into the registration process. See [End Users tab, page 79](#) for further details.
- ◆ **Forgotten your password?:** If users cannot remember their password, they can click **Forgotten your password?** They are redirected to a web page where they enter their email address. An email is sent containing a link to the Websense blueSKY portal where they must create a new password before being allowed to continue to authenticate.

As with all notification pages, you can tailor the default to meet your needs and use it to remind your users that they are using company resources that are governed by an acceptable use policy.

NTLM identification

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [NTLM registration page](#)
- ◆ [Further information about NTLM](#)
- ◆ [Access Control tab](#)

Select **NTLM transparent identification where possible** to use the Windows NT and LAN Manager authentication protocol (NTLM) identification for all users of this policy except those whose user agent types are known not to support it - for example, Firefox on Linux. Non-supported user agents are presented with the pre-login welcome page, and users can log on using the basic authentication mechanism.

NTLM registration page

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Further information about NTLM](#)
- ◆ [Access Control tab](#)

Users of policies where NTLM is selected must undergo an additional, once only, registration task to associate their NTLM credentials with their registered Websense blueSKY credentials. See [NTLM transparent identification, page 84](#) for further information. As with all notification pages, you can use the default page, customize it, or create your own.

Further information about NTLM

NTLM has evolved through numerous Windows and Windows NT versions. It provides a way for users to authenticate themselves with the company network.

NTLM identity

The NTLM identity is the domain\username with which users log on to their Windows PC; for example, MYDOMAIN\jsmith.

NTLM credentials

NTLM credentials include the NTLM identity (as defined above), the PC's identity, and a non-reversible encryption of the user's password. These are sent by the browser when a server (in this case a cloud service proxy) sends an NTLM challenge.

NTLM security implications

There are a number of security implications associated with the use of NTLM in Websense blueSKY. These are discussed below.

The NTLM credentials are being passed across an insecure Internet connection

NTLM is a secure protocol that does not carry the user's password, just a hash of the password, so intercepting the protocol does not reveal a user's credentials. To authenticate a user by validating a password hash, a network service must know the user's password. Websense blueSKY is outside of the company network, and so does not know the user's network password. For this reason, Websense blueSKY can use NTLM only to identify users, not to authenticate them. This limitation helps to preserve the security of the user's network passwords.

Transparent identification compared to basic authentication

Because NTLM does not require the user to actually authenticate with Websense blueSKY by entering a password, one might argue that it is less secure than basic authentication. This is not the case. Most Websense blueSKY users save their usernames and passwords in their browsers and therefore, if someone wanted to surf the Internet as another user, they can do so if they can access that user's PC. This is exactly the same situation as NTLM. To protect against this, in both cases, and with any product that provides web filtering, you should consider physical security and keyboard locking when users leave their desks to keep the network secure.

Limitations

1. Transparent identification does not authenticate; for example, it does not do password checking. It relies on the customer site having secure NT or Active Directory domains set up, along with physical security to stop unauthorized access to the company network or the users' computers.



Note

Although NTLM Identification works with Windows workgroups, it is not a recommended solution if you are concerned about security and correctly identifying end users.

2. You cannot use transparent identification for remote users. Remote users must be registered and must log on using their email addresses.
3. Users of non-Windows systems in a transparent identification policy still have to log on manually.

4. A browser that supports NTLM but is operating in a non-Windows environment (e.g., Firefox on a Linux platform), may exhibit strange behavior and may not work with a Websense blueSKY policy that is configured to use NTLM. Where possible, we attempt to identify such browsers by user agent type and send an authentication request rather than an NTLM challenge.
5. The existing Welcome page is not shown to users of NTLM-capable browsers in a transparent identification policy.

How NTLM works once users are fully configured

Fully configured means that users are registered with Websense blueSKY and their NTLM identities are known. See [End Users tab, page 79](#) for details on registering users, and [NTLM transparent identification, page 84](#) for details on NTLM identity.

1. Users start their browsers and try to visit a website.
2. Websense blueSKY checks the users' source IP address and applies the correct policy.
3. Websense blueSKY finds that transparent identification is enabled in the policy and initiates the NTLM conversation, during which the browser sends the NTLM credentials with no involvement of the users. Note that it is the local policy (i.e., the one identified by IP address) that determines whether NTLM is to be used.
4. Websense blueSKY finds the users' information in the policy by looking up the NTLM identity, and marks this connection as identified.
5. Websense blueSKY processes the original request as normal.

This all happens transparently, behind the scenes.

End Users tab

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [NTLM transparent identification](#)
- ◆ [Editing end-user registration pages](#)
- ◆ [Managing registered users](#)
- ◆ [Rules for policy association during end-user registration](#)

This screen is where all end-user registration configuration is performed. Registration is the method of getting user credentials into your Websense blueSKY account.

There are currently 3 methods of registering end users:

1. [Registering by invitation](#)

2. *Bulk registering end users*

3. *End user self-registration*

For (2) and (3) above, you must enter the email domains where the users' email addresses reside into the account or policy. See [Domains](#), page 52 for further information. For (1), users do not need an email address within your configured domains.

If you have chosen to use the directory synchronization feature to synchronize your LDAP-compliant directory (such as Active Directory) with Websense blueSKY as described in , you do not need to register end users at all. You can synchronize your organization's users with the cloud service instead. When you synchronize your directory, users are automatically registered with the cloud-based service.

Directory synchronization can include NTLM IDs. You can then enable NTLM identification on the Access Control tab. This allows your users to use the service immediately after synchronization, without their having to perform any self-registration actions or manual logon. If you enable NTLM identification but for some reason do not synchronize NTLM IDs from your directory, your users are required to complete the self-registration process, and then perform a second registration operation to associate their NTLM ID with their user account on the service. (See [NTLM transparent identification](#), page 84 for more information.)

If you don't want to use NTLM identification, you can configure the service to send invitations to all newly synchronized users. They can then complete self-registration process and log on using email address (or name) and password.

Through the directory synchronization feature, you have the option to notify new users that they are protected by the cloud-based service when they surf the web.

Registering by invitation

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

There may be users that you want to use your policy who do not have an email address within your email domains; for example consultants or contractors working at your location that you want to be bound by your Internet usage policy. You can invite these users to use the policy by selecting **Invite an End User** from the End Users tab.

Once you have added the end users' names, email addresses, and if available NTLM identification, Websense blueSKY sends them the registration email in the same way as if they had self registered. They click on the link and are asked to enter their password.

Field	Description
Name	Name of the user you want to invite to use the policy.
Email address	Email address of the user to invite.
NTLM Identity	The NTLM identity of the user, if available.
State	Enabled or disabled. If enabled, you can choose which block page to display for this user.

Bulk registering end users

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Bulk end-user registration simplifies the self-registration process by reducing it from 2 steps to 1. Rather than the end users visiting the portal and entering their names and email addresses into a form, you upload their names and email addresses in bulk, and Websense blueSKY automatically dispatches them email. The users can then register at stage 2, where they click a link in the email they receive and enter their password into the portal.

Uploading users' details

Click **Bulk register end-users** from the End Users tab when you want to upload end users' email addresses all at once. On the resulting screen, specify the file to upload and various other parameters:

Field	Description
Upload File	Browse to the text file to upload. See Bulk upload file format below.
Character Set	The character set of the file; this is normally either iso-8859-1 or Unicode.
Add New Users to Groups	You can add new users to a single or multiple groups by selecting them on this page. Alternatively you can specify group membership in the upload file.
File Contains NTLM Identities	Click if the file contains NTLM identities.
Replace details of existing users	Click if you want to replace a current record with this one.
Notification Email Address	Notification email address is the sender address of the registration email.
Invitation Email Language	The language variant of the registration email. To include language variants of this email, edit the End User Registration Email notification page. See Editing notification pages, page 47 .
Batch the Invitation Emails	Registration emails are batched to prevent your email servers being flooded by thousands of messages at once. You can specify the frequency.

Bulk upload file format

You can specify group membership in the uploaded file. The format of the file is shown below:

```
Name,EmailAddress,Groups
Fred Bloggs,fred.bloggs@acme.com,"Corporate Finance,All in Reading,"
```

Hans Bloggs, hans.bloggs@acme.de, All in Germany



Note

You can specify multiple groups, but because the field itself contains commas, you must enclose them in quotes.

The end of each line can be either a line feed, carriage return or both but you cannot mix them. For example, you cannot end one line with a carriage return and another with a line feed.



Note

If you are saving a file from Excel, do not Save As CSV (comma delimited) (*.csv), because this does not end lines consistently. Save As CSV (MS-DOS) (*.csv) instead.

The default notification template (end-user registration message) is available in HTML and TEXT. The version displayed to users depends on whether they use an HTML- or text-based email client.

Bulk upload results

After the file is uploaded, a status page is shown indicating whether any records were rejected and, if so, a link is displayed enabling you to download the rejected records, if desired.

Monitoring email dispatch

The status page also provides a link that lets you monitor the dispatch of registration messages.

The user management area also has a link to the upload status page. If there are multiple dispatches in progress, a list is shown.

End user self-registration

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

For individual end user self-registration, a user must have an email address on a domain that has been assigned to the policy or account. This allows you to control who can register to use each of your policies. Click **Add** on the End User tab to add domains to the policy.

Individual end-user self registration is a 2-stage process:

Stage 1

End users enter their name and unique email address.

They can also access this page by clicking **Register** on the default logon page. Once they have submitted their name and email addresses, Websense blueSKY sends them an email with a link, asking them to click it to confirm their registration.

Stage 2

Users click the link and are prompted for a password. From then on, if challenged by the proxy service, they can enter their email address and password to gain access to authenticated resources.

Directory synchronization

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [NTLM transparent identification](#)
- ◆ [End Users tab](#)
- ◆ [Set up authentication](#)

When you enable directory synchronization for your account, you can specify how users are assigned to policies. If you have multiple web policies, you can use group membership to assign users to policies. The assignment can be static (assigning a user to a policy only when that user is initially registered) or dynamic (changing policy assignment as group membership changes). This is all configured on the **Manage Directory Synchronization** page: see [Configure directory synchronization, page 30](#).

The End Users tab enables you to assign the current policy to a group or groups of synchronized users, overriding the default assignment:

1. Choose the **End Users** tab.
2. Under **Directory Synchronization**, click **Modify list of groups**.
3. Select the group(s) you want assigned to this policy.
4. Click **Submit**.

The effect of this action is to assign all members of the group to this policy.

NTLM transparent identification

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [NTLM registration page](#)
- ◆ [Further information about NTLM](#)
- ◆ [Access Control tab](#)



Note

For fully transparent NTLM identification, you should configure end users' browsers as described in the section 'Enabling browsers for NTLM transparent authentication' of the *Websense blueSKY Security Gateway Getting Started Guide*.

In order to access Websense blueSKY using NTLM transparent identification, some users are prompted to associate their NTLM credentials with their registration details the first time they access the service (or the first time transparent identification is enabled on their policy). This includes users who register themselves, are invited to register, or are bulk registered.



Note

If you are using directory synchronization and have synchronized NTLM IDs, users are not prompted for this information.

For non-directory users, the following process occurs one time:

1. The users start their browsers and try to visit a website.
2. Websense blueSKY checks the users' source IP address and applies the correct policy.
3. Websense blueSKY finds that transparent identification is enabled in the policy and initiates the NTLM conversation, during which the browsers send the NTLM credentials with no involvement of the users.
4. Websense blueSKY fails to find the users' NTLM information in the policy.
5. Websense blueSKY displays the NTLM registration page.
6. The users, if already registered, enter their email addresses and passwords and submit the form. If they are not already registered, they can click **Register**, also on this page, and are taken through the standard end-user self-registration process.
7. Websense blueSKY validates the usernames and passwords that are entered. If the validation fails, it re-displays the form.
8. If the validation succeeds, Websense blueSKY records the previously received NTLM identity against this user, and marks this connection as being identified.

Request processing continues as for a fully configured user.

Editing end-user registration pages

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

You can edit all end-user registration pages and the registration message to suit your requirements. The default pages include instructions to help users understand the process but these are limited for ease of editing.

Managing registered users

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

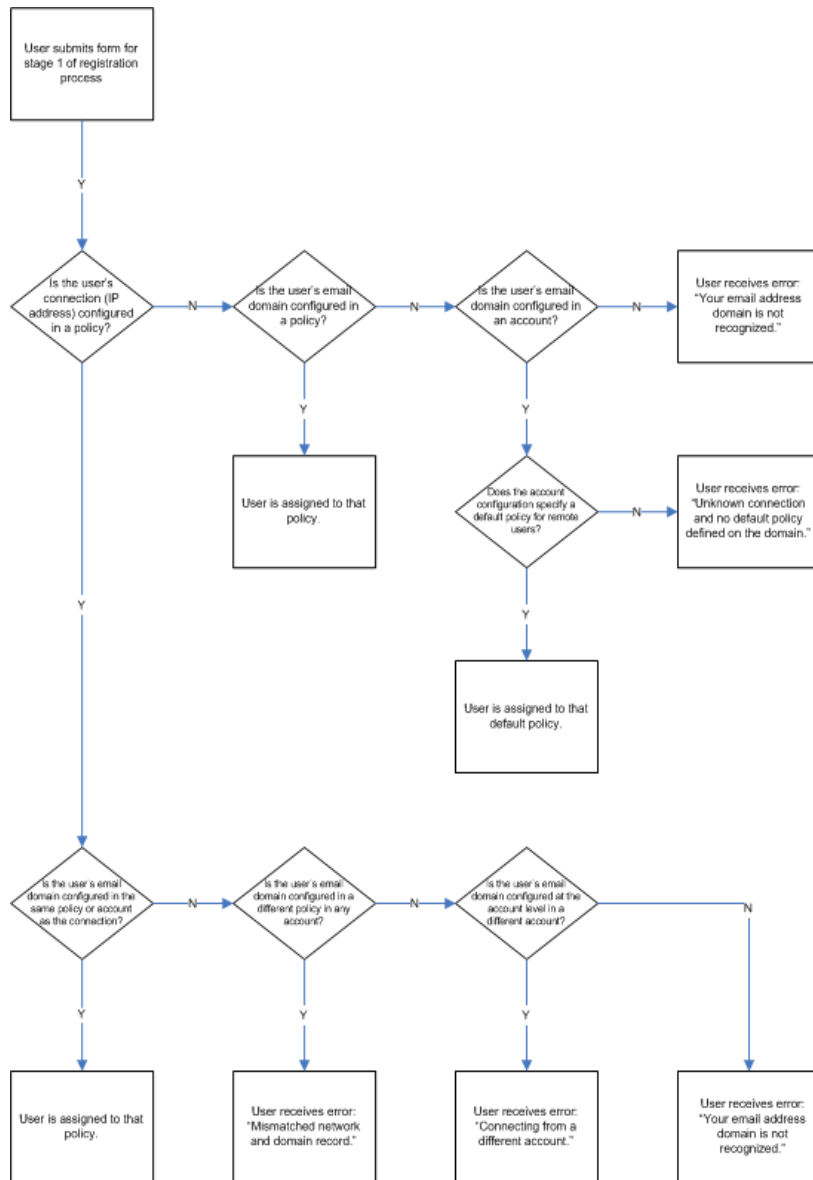
You can search the list of end users who are registering or have registered by clicking the link where the number of registered users is reported on the End Users tab. This page is the same as the account-level end users page, except that it applies changes at the policy-level.

From the search results page, you can select an individual user and modify his or her details. You can change a user's name (but not email address, because that uniquely identifies the user), delete the user, or block the user from accessing the service. Note that the service's self-registration feature means that deleting a user does not prevent that user from re-registering. However a blocked user is not able to re-register using the same email address.

Rules for policy association during end-user registration

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

The following diagram shows the rules that Websense blueSKY uses when determining with which policy a user is associated when they complete stage 1 of the registration process.



Web Categories tab

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Filtering actions](#)
- ◆ [Exceptions](#)
- ◆ [Filtering action order](#)
- ◆ [Category list](#)

Websense blueSKY includes dozens of website categories (see [Category list, page 92](#) for more details). 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".



Note

Websites can exist in one standard category, but multiple custom categories.

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 (see [Managing categories and filtering actions, page 87](#))



Managing categories and filtering actions

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

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—for example, **Internet Communication** is the parent category for **Web Chat**, **General Email**, **Organizational Email**, and **Text and Media Messaging**. 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.

A number of standard categories have icons next to them:

	<p>Privacy categories are marked with a padlock icon. This predefined group includes the following categories that may be subject to regulatory requirements:</p> <ul style="list-style-type: none"> • Financial Data and Services • Prescribed Medications • Education • Government • Health
	<p>Sites in Web 2.0 categories can contain highly dynamic content - for example, Web Chat and Internet Auctions.</p>

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. See [Filtering actions](#), page 88.
3. To apply the setting to all categories within the selected category, mark **Apply to all sub-categories**.
4. Click **Save**.

Filtering actions

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Exceptions](#)
- ◆ [Filtering action order](#)
- ◆ [Category list](#)

Each category has an **action** assigned to it. This is the action that Websense blueSKY takes in response to a user's Internet request. The action applies to all users of this policy unless exceptions are configured.

The available actions are:

◆ **Allow access**

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**

If you do not want websites to be blocked, select **Do not block**. This 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.

◆ **Block access**

This blocks access to websites in this category unless they exist in another category with a filtering action of **Allow access**. If the website exists in another category with the action **Do not block**, it is blocked under this category. When a site is blocked, you can choose a notification page to be displayed.

◆ **Confirm**

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.

Clicking Continue 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.

The default time can be changed on the **General** tab for the policy.

◆ **Use Quota**

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.

- If the user requests additional quota sites during a default **session** period (10 minutes by default), he can visit those sites without receiving another block page. If you are using per-category quotas, the user can visit only other sites in the same category without receiving another block page.
- **Total** quota time is allocated on a daily basis. Once it is used up, each user must wait until the next day to access sites in quota categories. The default daily quota allocation is set on the **General** tab for the policy. If you are using per-category quotas, the total quota time applies to each category and once it is used up for a particular category, a user can still use quota time in another category, if available.

The session length and total quota time available for each category depend on the options selected on the **General** tab. If you have defined per-category quotas, you can select **Use Quota** for a category on the **Web Categories** tab to change the total quota time and session length available to users in the policy for that category.

See [Using quota time to limit Internet access](#), page 90, for more information.

Using quota time to limit Internet access

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

When a user clicks Use Quota Time, she can view sites in any quota category until the quota session ends. The default quota session time (configured via the **General** tab of the policy) is 10 minutes.

Once the quota session ends, a request for a quota site results in another quota block message. Users who have not depleted their daily quota allocation can start a new quota session.

Internet applets, such as Java or Flash applets, may not respond as expected to quota time restrictions. Even if it is accessed from a quota-restricted site, an applet that runs within the browser can continue running beyond the configured quota session time.

This is because such applets are downloaded completely to a client machine and run just like applications, without communicating back to the original host server. If the user clicks the browser's Refresh button, however, Websense blueSKY detects the communication to the host server, and then blocks the request according to applicable quota restrictions.

Exceptions

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Filtering actions](#)
- ◆ [Filtering action order](#)
- ◆ [Category list](#)

Exceptions allow the default action for a category to be overridden for specified users and groups, and for defined time periods.



Note

If you set up an Allow exception, note that this overrides only the Block action on URL categories. It does not bypass any other actions.

On the Web Categories tab, the number of exceptions to the default filtering action is shown at the bottom of the page. Click a category to view exception rules that may apply.

On occasion you may want to add users to exceptions for policies they are not yet using or leave users in an exception list for a policy they no longer use. This allows you to set rules for users before they are moved between policies—for example, when policy assignment has been changed in an LDAP directory. If you add an unknown

user or if the user belongs to another policy, you receive a message to this effect. You can save rules that include users in other policies as well. These users are shown in the exception list with a red asterisk.

The exceptions table provides the following summary information about each rule:

- ◆ The name assigned to the rule.
- ◆ The category to which the rule applies. It always applies to the category you are viewing, but this indicates whether it applies to other categories. If there are multiple categories in the exception, click the link to see the category list. Note that if this is the case, the exception is also listed when you select the other category or categories.
- ◆ The users and groups to which the rule applies. If none are shown, it applies to all users of the policy.
- ◆ The time period to which the rule applies.
- ◆ The action for the rule, and whether it applies only to roaming users.
- ◆ The state of the exception rule – on or off. You can change the rule's state in this table by clicking the State switch.

To create an exception rule:

1. On the Web Categories tab, click a category name.
2. Click **Add exception**.
3. The rule **State** is set to ON by default, meaning the rule will be enabled for the users and groups you select. If you want to set up a rule but not enable it immediately, click the State switch to set it to OFF.
4. Enter a **Name** and **Description** for the rule.
5. Select the **Action** to apply from the drop-down list.
 - For the **Confirm** action, enter the time period for which a user who clicks Continue can access sites in the selected category or categories.
 - For **Use Quota**, any further options depend on the quota time configured on the policy's **General** tab. If the policy has an overall daily quota set, that quota applies to the exception and cannot be changed. If the policy is using the per-category daily quota, enter the total quota time and session length available to users and groups in the rule.
6. Select the **Time period** during which the rule is active.
7. For an exception that should be applicable to roaming users only, mark **Apply only when user is roaming**.
8. Select the category or categories to which the rule applies. To select multiple categories, use the **Shift** and/or **Ctrl** keys.
9. Enter or select the users and groups that will use the rule. You can also specify that the rule applies to all users and groups in the policy except the group you select.
10. Click **Submit**.

Filtering action order

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Filtering actions](#)
- ◆ [Exceptions](#)
- ◆ [Category list](#)

Websense blueSKY applies filtering actions in the following order:

- ◆ Security category blocking
- ◆ Application control blocking, File extension blocking, File type blocking, File Size blocking
- ◆ Standard or custom web categories: Allow access
- ◆ Standard or custom web categories: Confirm
- ◆ Standard or custom web categories: Quota
- ◆ Standard or custom web categories: Block access
- ◆ Standard or custom web categories: Do not block

When a per-time, per-user, or per-group exception also exists, it applies actions in this order:

- ◆ users with a time period defined
- ◆ users with no time period defined
- ◆ groups with a time period defined
- ◆ groups with no time period defined
- ◆ default with a time period defined
- ◆ default without a time period defined

Within each of these, Websense blueSKY uses the same order as the default.

Category list

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Filtering actions](#)
- ◆ [Exceptions](#)
- ◆ [Filtering action order](#)

Websense blueSKY uses the Master Database, which organizes similar websites (identified by URLs and IP addresses) into **categories**. Each category has a descriptive name, like Adult Material, Gambling, or Peer-to-Peer File Sharing.

The categories include the following:

- ◆ **Advanced Malware Command and Control** - focuses on outbound network transmissions from a compromised machine to a malicious command and control center
- ◆ **Advanced Malware Payloads** - focuses on inbound network transmissions of payloads intended to exploit a machine
- ◆ **Mobile Malware** - focuses on malicious websites and applications that are designed to run on mobile devices
- ◆ **Unauthorized Mobile Marketplaces** - focuses on websites that potentially distribute applications that are unauthorized by the mobile operating system manufacturer, the handheld device manufacturer, or the network provider. (Traffic to websites in this category may be a sign of a jailbroken or rooted device.)

You can also create your own, custom categories or import a custom category file (in CSV format) to group sites of particular interest to your organization (see [Custom categories, page 41](#)). Together, the Master Database categories and user-defined categories form the basis for Internet filtering.

Websense, Inc., does not make value judgments about categories or sites in the Master Database. Categories are designed to create useful groupings of the sites of concern to subscribing customers. They are not intended to characterize any site or group of sites or the persons or interests who publish them, and they should not be construed as such. Likewise, the labels attached to categories are convenient shorthand and are not intended to convey, nor should they be construed as conveying, any opinion or attitude, approving or otherwise, toward the subject matter or the sites so classified.

Protocols tab

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

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.

Protocol exceptions

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Exceptions allow the default action for a protocol to be overridden for specified users and groups of users. The number of exceptions to the default filtering action is shown at the bottom of the Protocols tab. Click a protocol to view exception rules that may apply to it.

The exceptions table provides the following information about each rule:

- ◆ The name assigned to the rule
- ◆ The protocol to which the rule applies. The rule always applies to the protocol you are viewing, but this column indicates whether the rule applies to other protocols. Note that if this is the case, this rule also appears when you select the other protocol or protocols.
- ◆ The users and groups to which the rule applies. If none are shown, the rule applies to all users of the policy.
- ◆ The action for the rule (**Allow** or **Block**)
- ◆ The status of the exception rule (**Enabled** or **Disabled**)

To create an exception rule:

1. Click **Add**.
2. On the Add Exception page, enter a **Name** (1 - 512 alphanumeric characters) and **Description** (1 - 1024 characters) for the rule.
3. Select the protocol or protocols to which the rule applies. To select multiple protocols, use the **Shift** and/or **Ctrl** keys. Use the arrow key to move a selection to the **Selected protocols** list.
4. Enter or select the users and groups for the rule:
 - Enter individual email addresses and use the arrow key to move the addresses to the **Selected users** list. Separate multiple addresses with a comma.
 - Select the user groups to which the rule applies and use the arrow key to move the groups to the **Selected groups** list.

You can also specify that the rule applies to all users and groups in the policy except the group you select.

5. Select the **Action** to apply from the drop-down list near the top of the page.
6. Mark the **Enabled** button to enable the rule for the users and groups you have selected.
7. Click **Save**.

To edit an existing exception, click the rule name link in the Protocol Exceptions list. The Edit Exception page appears showing the current settings for that rule.

To delete an exception, mark the check box to the left of the protocol name and click **Delete**.

Application Control tab

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Click the **Application Control** tab in the policy to configure social web controls for your end users.

To use the options on the Application Control tab, you must enable Real-time Security Classification on the Web Content & Security tab. See the [Web Content & Security tab, page 99](#).

Social web controls enable you to safely fine-tune access to popular sites within social media such as Facebook, Twitter, and YouTube. For each available site, you can specify whether users can access particular functions within the site, such as posting a comment or joining a group. For example, you may want to allow users to access their Facebook page, but not to upload photos or videos to the site.

The following filtering actions are available for social web controls:

- ◆ **Do not block.** This ensures that the function is not blocked, unless the category to which the parent site belongs has the action **Block access**. If you select Do not block for a function and the parent site is blocked on the Web Categories tab, a popup warning appears when you save your changes.
- ◆ **Block access.** This blocks the function and depending on the nature of the function, either displays the block page that you select, stops the function from working, or displays an error message.

The functions specific to each site are grouped together. If you set a particular filtering action for the parent application (for example, Twitter), it is also applied to all child functions for that application. You can subsequently change the action for individual functions.

Top-level sites related to the social web controls remain classified and filtered under their existing categories on the [Web Categories tab, page 87](#). For example, Facebook Chat is classified as Web Chat. You can only apply social web controls to a site if its corresponding web or custom category allows access or does not block the site.

If the top-level site is part of a category that has quota time applied to it, application controls are applied according to your configuration when the user is in a quota period. Similarly, if the site is in a category has the Confirm action applied to it, application controls are applied according to your configuration once the user has clicked Continue.

To configure application controls:

1. Select an application from the Applications list.

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

To select multiple applications, use the **Shift** and/or **Ctrl** keys. You can also use the drop-down menu above the Applications list to select or deselect all applications.

2. Select an **Action** for the category. Note that if you have selected a parent application (for example Facebook or Twitter), the action you select also applies to all the controls within that application by default.
3. If you have selected Block access, select a block page to display.
4. Click **Save**.

Application control exceptions

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Application Control tab](#)

Exceptions allow the configured action for an application control to be overridden for specified users, groups of users, and roaming users.

On the Application Control tab, the exceptions to the default configuration are listed at the bottom of the page. Click an application to view exception rules that may apply.

On occasion you may want to add users to exceptions for policies they are not yet using or leave users in an exception list for a policy they no longer use. This allows you to set rules for users before they are moved between policies—for example, when policy assignment has been changed in an LDAP directory. If you add an unknown user or if the user belongs to another policy, you receive a message to this effect. You can save rules that include users in other policies as well. These users are shown in the exception list with a red asterisk.

The exceptions table provides the following summary information about each rule:

- ◆ The name assigned to the rule.
- ◆ The application to which the rule applies. It always applies to the application you are viewing, but this indicates whether it applies to other applications. If there are multiple applications in the exception, click the link to see the application list. Note that if this is the case, the exception is also listed when you select the other application(s).
- ◆ The users and groups to which the rule applies. If none are shown, it applies to all users of the policy.
- ◆ The action for the rule, and whether it applies only to roaming users.
- ◆ The state of the exception rule – on or off. You can change the rule’s state in this table by clicking the State switch.

To create an exception rule:

1. On the Application Control tab, click a web application.
2. Click **Add exception**.

3. The rule **State** is set to ON by default, meaning the rule will be enabled for the users and groups you select. If you want to set up a rule but not enable it immediately, click the State switch to set it to OFF.
4. Enter a **Name** and **Description** for the rule.
5. Select the **Action** to apply from the drop-down list.
6. For an exception that should be applicable to roaming users only, mark **Apply only when user is roaming**.
7. Select the application to which the rule applies. To select multiple applications, use the **Shift** and/or **Ctrl** keys.
8. Enter or select the users and groups that will use the rule. You can also specify that the rule applies to all users and groups in the policy except the group you select.
9. Click **Submit**.

File Blocking tab

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Blocking by file extension](#)

Click the **File Blocking** tab in the policy to configure file blocking for categories that users are allowed to access according to your settings in the **Web Categories** tab. This capability allows your organization to restrict access to particular files from websites in some or all permitted categories, based on file type, extension, or size. For example, you could permit the category Sports, but block multimedia (audio and video) files from sites in the Sports category.

The following file blocking options are available:

- ◆ **File extension blocking.** This blocks files based solely on file extensions that you specify.

For example:

1. The General Email category has the Allow access action, but the file extensions “.zip” and “.rar” are blocked for the category.
2. An end user attempts to download a file with a file with a .zip extension (for example, “myfile.zip”).
3. The user receives a block page indicating that the download was blocked by file extension, because the “.zip” file extension is specifically blocked for this category.

For more details, see [Blocking by file extension](#), page 98.

Blocking by file extension

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [File Blocking tab](#)

1. On the File Blocking tab, click **Add Extensions**.
2. Enter the extension you wish to block. You can enter groups of extensions, separated by commas.



Note

If you include the period in the extension (for example, .jpg) it will be removed. Wildcards are not supported.

3. Set the file blocking **Rule State** to **Enabled**.
4. To configure blocking by file size:
 - a. Under **Blocking Options**, select **Block all files over ... KB**.
 - b. Define whether you want to block all files with this extension over a particular size that you enter or block files with this extension over a particular size but only in specific categories. You also have the option to block files in specific categories without regard to size.
5. To block files over a certain size in specific categories:
 - a. Select **Category specific blocking**.
 - b. Then, select **Block files in certain categories over ... KB**.
 - c. Fill in the size in kilobytes. Files over this size in the categories you choose will be blocked.
6. By default, a newly entered file extension is blocked for all categories. Click on



Note

Blocking by file size is not available for web traffic that has been handled by an appliance.

the red X next to the web category for which you wish to enable blocking by file size. You can also select the category and then choose the **Action** “Block when file size is ...”

7. You can select a category directly from the list, or enter text in the search box to locate the category you want. Click on the plus sign to the left of each category to view subcategories to which you can also apply blocking actions. If the parent and subcategory actions differ, an asterisk appears next to the parent category.

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:

- Web 2.0 categories
 - Privacy categories
 - All categories
8. Optionally, enter or select the users and groups to whom the file blocking applies. You can also specify that the file blocking applies to all users and groups in the policy except the group you select.
 9. Select the block page that will be displayed when this file extension is detected and blocked.
 10. Click **Save Changes**.

Web Content & Security tab

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Advanced analysis using real-time classification](#)
- ◆ [Antivirus file analysis](#)
- ◆ [Executable file analysis](#)
- ◆ [Analysis exceptions](#)

Click the **Web Content & Security** tab in the policy to configure advanced analysis options and exceptions.

These options support the analysis of web traffic as it flows through the Websense blueSKY proxy. Only sites that are not already blocked, based on the active policy, are analyzed.

Advanced analysis uses the to provide the following:

- ◆ Real-Time Content Classification
- ◆ Real-Time Security Classification
- ◆ Antivirus File Analysis
- ◆ Advanced Detection File Analysis
- ◆ File Type Analysis
- ◆ Executable File analysis and blocking

Real-time classification consists of:

- **Real-Time Content Classification** categorizes content from URLs that are not in the Websense Master Database and from sites with dynamic Web 2.0 content, as identified by Websense Security Labs. This analysis returns a category for use in filtering.

- **Real-Time Security Classification** analyzes web pages in real time to discover malicious content providing protection from malware and other threats, and returns a category for use in filtering.

Antivirus file analysis applies 2 methods of inspection to detect inbound security threats.

- **Antivirus File Analysis** analyzes files using traditional antivirus (AV) definitions to find virus-infected files.
- **Advanced Detection File Analysis** analyzes files using Websense advanced detection techniques to discover malicious content, such as viruses, Trojan horses, and worms, returning a threat category for policy enforcement.

When either of the above is enabled, you can also optionally:

- **Analyze rich Internet applications**, such as Flash files, to detect and block malicious content.

Outbound file analysis is enabled by default, and cannot be switched off.

File Type Analysis Options determine which types of files are analyzed for malicious content, including unrecognized files. Individual file extensions may also be specified. You can specify the maximum file size to analyze (default 10 MB). Larger files pass through the proxy without analysis.

Selecting an option in this section enables file type analysis only for content from sites with elevated risk profiles.

[Executable file analysis, page 103](#), enables you to protect your organization from inbound or outbound executables.

[Analysis exceptions, page 103](#), are lists of URLs that are always analyzed or never analyzed. The type of analysis to always or never perform is specified per URL or group of URLs.

Advanced analysis using real-time classification

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Antivirus file analysis](#)
- ◆ [Executable file analysis](#)
- ◆ [Analysis exceptions](#)

When a URL is requested, real-time content classification is performed if:

- ◆ The URL has not already been blocked by the active policy
- ◆ The URL is not in the Websense Master Database, or
- ◆ The URL is a Web 2.0 site, as identified by Websense Security Labs

The category that is determined by content classification is forwarded to Websense blueSKY for policy enforcement.

Content classification provides high value because a significant majority of web content changes rapidly. In addition, the Internet hosts a large amount of user-generated content, such as that found on social-networking sites. Content classification analyzes this content at the moment it is needed, when it is requested.

Optionally, you can select **Analyze links embedded in Web content** as part of content classification. Such analysis can provide more accurate categorization of certain types of content. For example, a page that otherwise has little or no undesirable content, but that links to sites known to have undesirable content, can itself be more accurately categorized. Link analysis is particularly good at finding malicious links embedded in hidden parts of a page, and in detecting pages returned by image servers that link thumbnails to undesirable sites.

When you select **Real-Time Security Classification**, Websense blueSKY performs web page content analysis to discover security threats and malicious code for sites with elevated risk profiles, including Web 2.0 sites, as identified by Websense Security Labs.

You must enable Real-Time Security Classification to use the options on the Application Controls tab. See [Application Control tab, page 95](#).

To configure advanced analysis classification settings:

1. Go to **Web Security > Policy Management > Policies** and select the policy you want to edit.
2. Click the **Web Content & Security** tab.
3. To enable content security, select **Real-Time Content Classification**.
4. Select **Analyze links embedded in Web content** to include embedded link analysis in content categorization. Requests that are blocked as a result of link analysis are logged and can be viewed in Analysis Activity reports.
5. To enable security analysis, select **Real-Time Security Classification**. Real-time security classification applies only to sites with elevated risk profiles.
6. When you are finished, click **Save**.

Antivirus file analysis

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Advanced analysis using real-time classification](#)
- ◆ [Executable file analysis](#)
- ◆ [Analysis exceptions](#)

Antivirus file analysis inspects files that users attempt to download or open remotely for viruses and other malicious content. File analysis returns a category to Websense blueSKY filtering for policy enforcement.

There are 2 types of file analysis. They can be used together.

- ◆ **Antivirus file analysis** uses antivirus definition files to identify virus-infected files.
- ◆ **Advanced detection** applies techniques developed by Websense to discover known and emerging threats, including viruses, Trojan horses, worms, and others.

Enabling either of these options causes the cloud service to analyze only sites with elevated risk profiles.

You can configure the specific types of files to analyze under **File Type Analysis Options**. Note that executable file analysis is configured separately (see [Executable file analysis](#), page 103).

**Note**

If file analysis is configured to include multimedia files, when the streaming media is buffered and analyzed, the connection to the server may time out. In such cases, the best remedy is to create an analysis exception for that site. See [Analysis exceptions](#), page 103.

Both of the above file analysis methods are applied to outbound files by default. This ensures that viruses and other malicious content cannot be sent from your network. When bot or phone home traffic is detected, it is also categorized and blocked. This traffic is also logged, so you can run a report to obtain a list of the infected computers in your network.

To configure antivirus file analysis options:

1. On the Web Content & Security tab, select **Antivirus File Analysis - Inbound** to enable file analysis with antivirus definitions. This option enables file analysis on files from uncategorized sites and files from sites with elevated risk profiles, including Web 2.0 sites, as identified by Websense Security Labs.
2. Select **Websense Advanced Detection File Analysis - Inbound** to enable advanced detection file analysis. This option enables file analysis on files from uncategorized sites and files from sites with elevated risk profiles, including Web 2.0 sites, as identified by Websense Security Labs.
3. Select **Rich Internet Application analysis** to analyze Flash files for malicious content.
4. Click **Save**.

File type analysis options

To specify the types of files to analyze, select file types under **File Type Analysis Options**. As a best practice, analyze all suspicious files, as identified by Websense

Security Labs, and all unrecognized files. Using this option enables file type analysis only for sites with elevated risk profiles.

To always analyze files having a specific extension, under **Analyze these file extensions**, enter the extension in the entry field and click **Add** or press **Enter**. You can enter multiple extensions, separated by commas. For example, enter gz, cad, or js.

- ◆ To edit an existing file extension, you must delete it, and add it again with the changes that you want.
- ◆ To remove an extension from the list, select the extension or extensions from the list, and click **Delete**. To select multiple extensions, select each extension while pressing the **Ctrl** or **Shift** key.

To set the maximum file size of file types to be analyzed (default 10 MB), go to **Maximum file size to analyze**, and enter the size in megabytes. Files larger than the specified size are not analyzed.

When you're done, click **Save**.

Executable file analysis

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Advanced analysis using real-time classification](#)
- ◆ [Antivirus file analysis](#)
- ◆ [Analysis exceptions](#)

You can choose to protect your organization from inbound executables.

If you choose to analyze executable file downloads, you can block executable files by category on the [File Blocking tab](#). Use the File Blocking tab to configure the notification page presented to the user when an executable download is blocked.

Executable file download analysis applies only to downloads from sites with elevated risk profiles.

Analysis exceptions

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:


- ◆ [Advanced analysis using real-time classification](#)
- ◆ [Antivirus file analysis](#)
- ◆ [Executable file analysis](#)

Analysis exceptions are lists of trusted or untrusted sites (host names) that are **never analyzed** or **always analyzed**. The type of analysis to never or always perform is specified per host name or group of host names.

Use the **Always Analyze** and **Never Analyze** lists to refine the advanced analysis offered by the cloud service. When real-time content classification, real-time security classification, or antivirus file analysis options are enabled, sites on the **Always Analyze** list are always analyzed, and sites on the **Never Analyze** list are never analyzed.

Use the Never Analyze list with caution. If a site on the list is compromised, Websense blueSKY does not analyze the site and cannot detect the security problem.

To add sites to the Always Analyze or Never Analyze lists:

1. Click the **Add Host name** button .
Enter the host name only, for example, **thissite.com**. It is not necessary to enter the full URL.
Be sure to enter both the domain and the extension. For example, **thissite.com** and **thissite.net** are distinct entries.
2. Click the Add icon  to add the host name to the list.
A site can appear in only 1 of the 2 lists.
3. To delete a site from a list, click the Delete icon  next to the host name.

SSL Decryption tab

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Enabling SSL decryption](#)
- ◆ [Configuring SSL decryption for web categories](#)
- ◆ [Bypassing SSL decryption for specific sites](#)

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

When you enable SSL decryption, HTTPS traffic is inspected to ensure the correct notification or authentication page, if applicable, is delivered to the end user. See [Enabling SSL decryption, page 105](#).

If available in your account, you can define SSL decryption for analysis of specific web categories, enabling HTTPS sites to be checked for malware and other web threats, and to receive the intended dispositions for their categories. See [Configuring SSL decryption for web categories, page 105](#).

You can also maintain a list of host names for which SSL decryption is not performed. See [Bypassing SSL decryption for specific sites](#), page 106.

Enabling SSL decryption

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

SSL (Secure Sockets Layer) is the industry standard for transmitting secure data over the Internet. It is based on a system of trusted certificates issued by certificate authorities and recognized by servers.

When you enable SSL decryption for Websense blueSKY users, 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, or the [Pre-logon welcome page](#), page 76 for authentication.

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**.



Note

You should also define a certificate when you add an appliance and install that certificate on users' machines, in order to avoid browser warnings regarding SSL termination block, authentication, or quota/confirm operations. See [Generating a certificate](#), page 64.

Configuring SSL decryption for web categories

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

When SSL decryption is enabled to handle encrypted traffic, use the SSL Decryption Categories settings to specify categories of websites for which security analysis is performed.

This option applies only to elevated risk categories and to Websense standard categories, not custom categories.

All categories are disabled for decryption by default. If you enable one or more categories for decryption, you must also enable at least one of the analysis options on

the [Web Content & Security tab, page 99](#), since these options define the types of security analysis that takes place. If you do not enable any of these options on the Web Content & Security tab, the categories you select are decrypted to enable the correct notification pages to be served, but not analyzed.

All categories have a shield icon displayed next to them. When the shield contains a green tick, the category is enabled for SSL decryption.

To set up SSL decryption for one or more web categories:

1. Under **SSL Decryption Categories** on the SSL Decryption tab, 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
- Web 2.0 categories

2. Select **Decrypt**.
3. Click **Submit**.

Bypassing SSL decryption for specific sites

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

The SSL Decryption Bypass option enables you to define specific websites that are not subject to decryption as they flow through the proxy. Some websites may include personal identification information that should not be decrypted. In order to avoid liability for inspecting this type of information, you may want to specify some or all of these sites for decryption bypass. The selected sites will not be decrypted even if the category or categories that the sites belong to are selected for SSL analysis.

End users can determine that the website they are viewing is not decrypted by checking who has issued the certificate for that site. If the certificate was issued by Websense Inc., traffic to the site has been decrypted.

To set up the bypass of SSL decryption for certain sites:

1. Under **SSL Decryption Bypass** on the SSL Decryption tab, enter the site's host name in the entry field and press **Enter**. You can enter multiple host names, separated by commas.

You can use the asterisk wildcard in a host name, for example *.google.com.

To edit an existing site, click the name under the entry field. Press **Enter** to save your changes as a new entry in the site list. To discard your changes, press **Esc**.

To remove a site from the list, click the Delete icon next to the host name.

2. Click **Submit**.

7

Reporting

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Downloading report results](#)
- ◆ [Reporting periods](#)
- ◆ [Account Summary report](#)
- ◆ [Categorized reports](#)
- ◆ [Web reports](#)
- ◆ [Cloud Service reports](#)
- ◆

Websense blueSKY reporting functionality provides you with the tools to report on security and usage.

- ◆ Click **Home** > **Reports** to generate an account summary report. If you have directory synchronization enabled for your account, you can also generate synchronization statistics for the service.
- ◆ Click **Web Security** > **Reports** to see the web filtering reports that are available. Depending on your subscriptions, you may see: Volumes, Browsing Times, Real Time Scanning, Web 2.0 Applications, Protocols, and Authentication and Endpoint.

For more information on these specialized reports, refer to [Categorized reports, page 111](#). For details of specific web reports, see [Web reports, page 116](#).

Reporting allows you to:

- ◆ Monitor service performance
- ◆ Monitor traffic volumes and patterns for capacity planning purposes
- ◆ Identify areas for potential future investment in other communication technologies
- ◆ Enforce your web acceptable use policy

- ◆ Help problem isolation and resolution



Note

Unless you have all services, you receive only the reporting functionality specific to those services for which you are licensed.

All reports are generated in real time using the Websense blueSKY portal. Most include charts and tables that are presented in an easy to read, printable format.



Note

For larger accounts, where a lot of data is to be retrieved, the reports may take some time to generate. As soon as the relevant data has been retrieved it is displayed while the remainder of the report is being compiled.

Commonly-used report criteria can be saved for easy access. For more information, see [Saving reports](#), page 112. Saved reports can be scheduled for regular delivery to one or more recipients as described in [Scheduling categorized reports](#), page 113.

Reporting periods

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Reports can be generated for periods of hours to years. When accessing a report, you can drill down from within the report to a shorter time period. For example, an email volumes report for 7 days returns a table of volumes by day and a corresponding bar chart. By clicking a link on the relevant day on the table or chart, the report drills down and provides an hourly table and chart for that day. This allows not only the creation of management reports, but also reactive tracking of day-to-day issues.

You can select the reporting period from the drop-down list or you can click **more** to select absolute From and To dates and times. The available dates and times are dependent on the type of report and the availability of the data.

Downloading report results

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

On each report, you have the option to download the data as a PDF or CSV file.



Note

You can also download charts as image files or in PDF format. To download a chart, right-click the chart and select the format to download (PDF, PNG, or JPEG).

Downloading a CSV file

You can download the statistics for the majority of reports as a comma-separated values (CSV) file. This allows you to import it into a third-party application, such as Microsoft Excel, for viewing and manipulation. On each table of results, click **Download CSV** to begin the download.

Downloading a PDF file

Report results can be output to Portable Document Format (PDF) for easy distribution or printing. The PDF report is generated by clicking the **Download PDF** button on a table of results.

Account Summary report

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Scheduling Account Summary reports](#)

The Account Summary report is a combination of reports that can be obtained elsewhere in this section of the portal. Select the time period, click **Go**, and you are presented with a summary of the web traffic that has been processed for your account during the selected time period. (If you have a lot of mail flowing through the system, this may take a while.) The report is organized by section and preceded by a table of contents with hyperlinks into specific data. Click the links to view the report, or scroll down the page using the scroll bar.

Scheduling Account Summary reports

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

If you would like non-graphical versions of the Account Summary reports to be sent to one or more email addresses on a regular basis:

1. Select **Home > Reports > Account Summary**.
2. Click the **click here** link on the Account Summary Report page to set up report delivery.
3. Enter one or more email addresses to which you want the report sent.

If you enter an address with a domain not registered to the account, a warning appears when you save the schedule. Click **OK** on the warning to accept the address.

4. Set up a subscription schedule by specifying one of the following delivery periods for your reports:

- daily
- weekdays
- weekly
- every other week (biweekly)
- monthly (the default option)

If you want to stop the a scheduled report temporarily, select **suspend delivery**.

5. Click **Save**.

Your schedule details are then shown on the Account Summary page. You can edit or delete your details from the **click here** link.



Note

You must renew your subscription to the Account Summary report every 3 months or your subscription expires.

Printing Account Summary reports

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

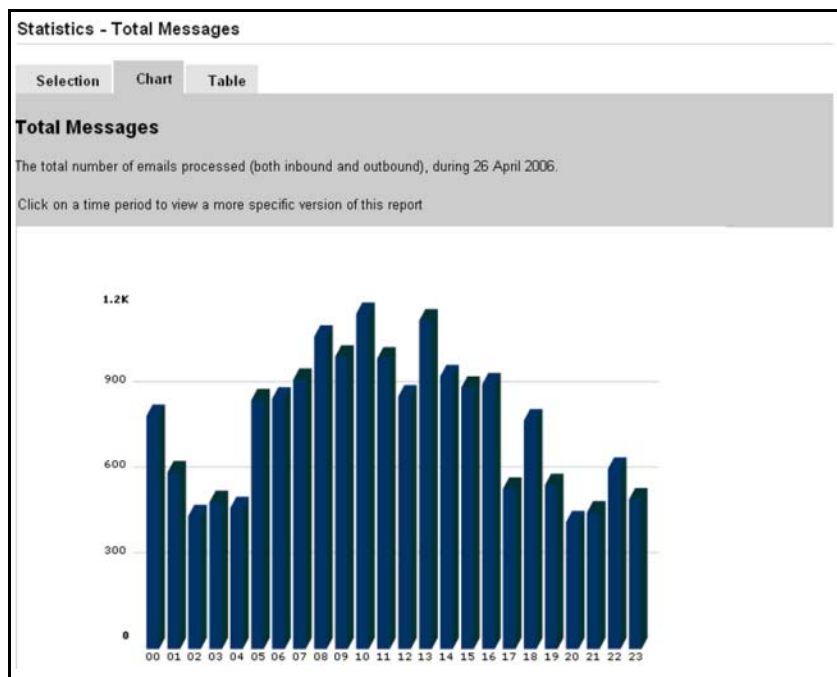
Once you have generated the Account Summary report, click **Click here to print this page** to get a printer-friendly version of the report. After a few seconds a printer selection dialog box appears.

Please leave plenty of time for the graphics to appear before printing. We recommend that you select “Landscape” format.

Viewing detailed information

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

To view detailed daily information, click the relevant bar in the chart or the date in the table. The result of doing so is shown below.



You can expand each section in the Account Summary report in this manner. By doing so, you are actually launching a categorized report query. See [Categorized reports](#), page 111 for further details.

Categorized reports

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Saving reports](#)
- ◆ [Scheduling categorized reports](#)

There are many reports available so they are categorized into groups. The report groups are shown in the navigation pane under **Web Security > Reports**.

The reports you see depend on your subscriptions.

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.

**Note**

If your account is enabled for filtered reporting, you may only be able to view reports that filter on certain policies and/or Web groups. See [Permissions definitions](#), page 13.

When you select a report, you are shown a list of the time periods for which the report is available. Alternatively you can select a specific time period (from and to) for the report by clicking **more** next to the period list.

To make selection from some criteria lists easier, you can expand the list to appear in a larger window by repeatedly clicking on the **Grow list** link.

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.

Report results

Most report results are displayed in chart and table format in the relevant screen. Note that not all reports are available in both formats.

Drilling down

Many of the reports contain links to more detailed reports. For example, for time-based reports, clicking the chart column or data table entry for a day generally displays the hourly report for that day, using any filtering criteria that applied to the original report.

Some reports allow you to drill down into the data in a more flexible way. If this is the case, there is a drop-down list above the chart and data table listing the available views. Select the view required from the list and then click the chart or table to display the new report.

Saving reports

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

◆ [Scheduling categorized reports](#)

You can choose to save any categorized report. Use this option to identify the reports you generate most frequently and want to be able to locate quickly.

To see the list of reports that you have saved, select **Reports > Saved Reports**.

To save a report:

1. Under **Reports**, select the report you want.
2. Use the **Selection** screen to enter your report criteria as described in [Categorized reports, page 111](#).
3. Click **Save report**.
4. Enter a name for the report, and click **Save**.

The Saved Reports list is displayed, and the report you entered is now listed.

As well as accessing the report from this screen, you now have the option to delete the saved report or schedule it for regular delivery.

Scheduling categorized reports

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Related topics:

- ◆ [Saving reports](#)

You can run reports as they are needed, or you can define a schedule for running one or more saved reports.

Reports generated by scheduled jobs are distributed to one or more recipients via email. The reports can be in HTML, PDF, or CSV format. There is a limit on the number of reports you can schedule for delivery: the Saved Reports list displays the remaining number you can schedule in addition to any existing deliveries.



Note

You cannot schedule reports that have defined start and end dates, or that span periods of less than 24 hours.

To schedule a report:

1. Select **Reports > Saved Reports**.
2. You can schedule an existing saved report by clicking the report you want to schedule on the Saved Reports list. If you do this, skip to step 5 below.
Otherwise, to create a new report for scheduling, click the **Generate a new report** link. The page that appears includes only reports that are eligible for scheduling.
3. Create and save your report as described in [Saving reports, page 112](#).
4. On the Saved Reports list, click the name of your new report.
5. Click **Schedule email report**.

6. Enter the email address of the report recipient. Multiple email addresses should be separated by commas or spaces.

If you enter an address with a domain not registered to the account, a warning appears when you save the schedule. Click **OK** on the warning to accept the address.

7. Enter a subject for the report email, and the text you want to appear in the body of the email.
8. Select the report format.
9. Set one of the following delivery periods for your reports:
 - daily
 - weekdays
 - weekly
 - every other week (biweekly)
 - monthly (the default option)

If you want to stop the a scheduled report temporarily, select **suspend delivery**.

10. Click **Save**.

You are returned to the Saved Reports list. Reports that have been scheduled display the recipient list in the **Email to** column. Click an item in this column to open the schedule, where you have the option to edit or delete the report delivery.

Cloud Service reports

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

The Cloud Service reports provide data that relates to directory synchronization and to end user message report subscriptions.

Cloud Service reports can be saved and scheduled in the same way as the categorized reports. For more information, see [Saving reports, page 112](#) and [Scheduling categorized reports, page 113](#).

Directory synchronization reports

If you have directory synchronization enabled on your account, you can view and print reports on the portal that show the history of directory synchronizations, including high-level statistics on success/failure and numbers of items synchronized.

1. Select **Home > Reports > Services**. The following screen appears:

Cloud Services Report

Selection Chart Table

Please select a report, a time period, and any required filters and click on *Generate report*. Note that if nothing is entered or no selection made for any particular filter then that filter will not be applied.

Show Synchronization History Log - connection history (limited to 1,000 rows)

during the last 6 hours more...

Generate report Save report

2. From the **Show** drop-down list, select a report to show:

Report	Description
Synchronization History Log	The history log provides a connection history for the specified period, up to 1000 rows.
Synchronization Time Summary	The time summary provides a list of the 20 longest synchronization times.

3. From the **during** drop-down list, select the time period for the report. Click **more** to select a specific date or time.



Note

The 'last 6 full hours' period does not include a synchronization just performed. You must wait for the hour to pass for it to appear in this report. You can view the very latest synchronization history in the Manage Directory Synchronization page on the **Setup** tab.

4. Click **Generate report**. Following is a sample Synchronization History Log:

Selection Chart Table

Synchronization History Log

connection history (limited to 1,000 rows), during the last 7 days.

Date (UTC)	SourceIP	Type	Status	Additions	Deletions
2008-10-21 10:56:53	10.5.21.32	test	200 OK		
2008-10-21 10:57:21	10.5.21.32	Addresses	200 OK		
2008-10-21 10:59:15	10.5.21.32	test	200 OK		
2008-10-21 10:59:54	10.5.21.32	Addresses	200 OK	27	0
2008-10-21 11:01:13	10.5.21.32	Groups	200 OK	8	0
2008-10-21 11:01:43	10.5.21.32	Users	403 SQL oommand failed after 1 attempts: DBD::mysql::st execute	0	0
2008-10-21 13:07:06	10.5.21.32	Groups	200 OK	8	0
2008-10-21 13:07:18	10.5.21.32	Users	403 SQL command failed after 1 attempts: DBD::mysql::st execute	0	0
2008-10-21 13:10:19	10.5.21.32	test	200 OK		
2008-10-21 13:10:40	10.5.21.32	Groups	200 OK	0	0
2008-10-21 13:10:50	10.5.21.32	Users	200 OK	0	0
2008-10-22 09:16:14	10.5.21.32	test	200 OK		
2008-10-22 09:16:39	10.5.21.32	Addresses	200 OK	27	0
2008-10-22 09:16:52	10.5.21.32	Groups	200 OK	0	0
2008-10-22 09:17:05	10.5.21.32	Users	200 OK	0	0

You can download the report to a CSV or PDF file. You can also print the report.

Browse Time reports

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

It is not possible to accurately tell exactly how long someone has spent browsing a Web site. A user might download a large Web page and then spend 10 minutes reading it, during which time there are no further requests or uploads and downloads of data. For the purposes of producing browse time reports, we make a number of assumptions.

All requests are tracked and browsing times are measured by the number of distinct minutes spent browsing. Whether one or one hundred requests are processed by Websense blueSKY, for a user, in any 1 minute period, that user is assumed to have been browsing for 1 minute. When a user requests a Web page, this registers as one minute. If he/she then made 10 further clicks to find the page with the information on it that was required, but all of these clicks were made within the next minute, this shows that he/she has been browsing for another 1 minute. If the user then spent 10 minutes reading the page before making another request, this would show in another 1 minute session. For this period the time spent browsing is assumed to be 3 minutes.

Web reports

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

To access a web report:

1. Go to **Web Security > Reports**.
2. Select a report category from the navigation pane.
3. Select a report from the **Show** drop-down list.

The sections below show the reports that are available.

- ◆ *Application Control reports*
- ◆ *Browsing Times reports*
- ◆ *Real-Time Analysis reports*
- ◆ *Volumes reports*



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.

Application Control reports

Report	Available Periods	Formats	Description
Major Application Groups	Hourly Daily	Chart Table CSV Link PDF Link	Displays the total number and sizes of requests to the most frequently-visited Web 2.0 sites available for application controls – Facebook, LinkedIn, Twitter, YouTube etc.
Minor Application Types	Hourly Daily	Chart Table CSV Link PDF Link	Displays the total number and sizes of requests to the most frequently-accessed application controls within sites such as Facebook, LinkedIn, Twitter, and YouTube.
Top Users of Major Applications	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Displays the most frequent users of application controls – for example Facebook, LinkedIn, and Twitter.
Top Users of Minor Applications	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Displays the most frequent users of application controls within sites such as Facebook, LinkedIn, and Twitter – for example Facebook Chat or YouTube commenting.
Individual User Investigation Report	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Displays a specified user's requests to major and minor application types over a defined period of time.

Browsing Times reports

Report	Available Periods	Formats	Description
Browsing Times by Category	Hourly Daily	Chart Table CSV Link PDF Link	Browsing times of the most frequently-visited categories
Browsing Times by Disposition	Hourly Daily	Chart Table CSV Link PDF Link	Browsing times for each disposition
Browsing Times by Policy	Hourly Daily	Chart Table CSV Link PDF Link	Browsing times for the most active policies
Browsing Times by Site	Hourly Daily	Chart Table CSV Link PDF Link	Browsing times of the most frequently-visited sites
Browsing Times by Time	Hourly Daily	Chart Table CSV Link PDF Link	Browsing times varying over time
Browsing Times by User	Hourly Daily	Chart Table CSV Link PDF Link	Browsing times of the most frequent users

Real-Time Analysis reports

Report	Available Periods	Formats	Description
Details of Security Blocked Requests	Minutes Hourly Daily	Chart Table CSV Link PDF Link	Request websites blocked by security type
Malware Detail	Hourly Daily	Chart Table CSV Link PDF Link	Details of all uploaded and downloaded malware in the specified period. You can drill down to see which users are affected.
Malware Volumes	Hourly Daily Monthly	Chart Table CSV Link PDF Link	The total number of inbound and outbound requests detected as containing malware by all techniques including ThreatSeeker.
Security Risk Volumes by Site	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Displays the total number of requests by site that were blocked due to the detection of dangerous content. You can drill down to see more details for a particular site.
Security Risk Volumes by Time	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Displays the total number of requests over a defined time period that were blocked due to the detection of dangerous content.
Security Risk Volumes by User	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Displays the total number of requests by the most frequent users that were blocked due to the detection of dangerous content. You can drill down to see more details for a particular user.
Web 2.0 Volumes by Category	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Displays the total number and sizes of requests to the most frequently-visited categories classed as Web 2.0 sites.

Report	Available Periods	Formats	Description
Security Classification of Analyzed Requests	Hourly Daily Monthly	Chart Table CSV Link PDF Link	Displays the total number and sizes of requests that have been assigned to categories due to real time security analysis.
Spyware Activity Summary	Hourly Daily Monthly	Table CSV Link PDF Link	Summarizes requests to botnet and spyware sites over a defined time period.
Detail of Real Time Blocked Requests	Minutes Hourly Daily	Table CSV Link PDF Link	Displays all requests blocked by real-time classification for a particular user over a defined time period.
Top Web 2.0 Users	Hourly Daily	Chart Table CSV Link PDF Link	Lists the most prolific users of Web 2.0 sites over a defined time period. You can drill down to see more details for a particular user.
Web 2.0 User Activity Summary	Hourly Daily	Table CSV Link PDF Link	Summarizes all requests to Web 2.0 sites made by a particular user over a defined time period.

Volumes reports

Report	Available Periods	Formats	Description
Overall Volumes	Minutes Hourly Daily	Chart Table CSV Link PDF Link	Request volume varying over time
Volumes by Category	Hourly Daily	Chart Table CSV Link PDF Link	Request volumes and sizes of the most frequently-visited categories
Volumes by Disposition	Hourly Daily	Chart Table CSV Link PDF Link	Request volumes and sizes for each disposition

Report	Available Periods	Formats	Description
Volumes by Policy	Hourly Daily	Chart Table CSV Link PDF Link	Request volumes and sizes for the most active policies
Volumes by Protocol Group	Hourly Daily	Chart Table CSV Link PDF Link	Request volumes and sizes of the most frequently used protocol groups
Volumes by Protocol	Hourly Daily	Chart Table CSV Link PDF Link	Request volumes and sizes of the most frequently used protocols
Volumes by Site	Hourly Daily	Chart Table CSV Link PDF Link	Request volumes and sizes of the most frequently-visited sites
Volumes by Time	Hourly Daily	Chart Table CSV Link PDF Link	Request volumes and sizes varying over time
Volumes by User	Hourly Daily	Chart Table CSV Link PDF Link	Request volumes and sizes of the most frequent users
Browsing Times by User	Hourly Daily	Chart Table CSV Link PDF Link	Browsing times of the most frequent users
Daily Summary	Daily	Table CSV Link PDF Link	Request summary data by day (limited to 1,000 rows)
Detailed Summary	Minutes Hourly Daily	Table CSV Link PDF Link	Detailed request summary data (limited to 1,000 rows)
Exception Request Log	Minutes Hourly Daily	Table CSV Link PDF Link	Request exception log (limited to 1,000 rows)

Report	Available Periods	Formats	Description
Web Performance	Minutes Hourly Daily	Table CSV Link PDF Link	Detailed data for Web response times
User Agents by Volume	Minutes Hourly Daily	Table CSV Link PDF Link	Authentication requests and total requests for all user agents.

8

Audit Trails

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

The following audit trails are available:

- ◆ *Configuration audit trail* - Lets you examine the configuration audit database for your account. This gives you visibility into all of the configuration changes that have been made on the account. Access this by choosing **Account Settings > Audit Trail**.

Configuration audit trail

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

The configuration audit trail provides visibility of all policy changes. You can access it by selecting **Account Settings**, then clicking **Audit Trail**. Searches are by user and the change made within a defined date range.

Results indicate the changes that meet the search criteria, when they were made, and by whom.

Click **Export to CSV** to export the results of your audit trail search. This creates a file named `audit_trail.csv`; you can either open the file, save the file with the default name, or save the file with a new name.

9

Standard Web Configuration

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

The Websense blueSKY service provides a standard configuration for all Web accounts. The settings for the standard configuration are described below, as well as the reasoning behind the settings. As an administrator, you can customize policy settings to suit your needs. Do this by clicking **Web Security > Settings**, then following the instructions in [Configuring Web Security, page 41](#).

The first 6 tables in this section represent the options on the **Web Security > Settings** menu, and the final table displays the policy management options. Column 4 suggests various use cases for changing the standard setting.

Custom Categories	Standard setting	Reason for standard setting	Consider changing setting if...
Custom categories	There are no custom categories by default.		You want to create your own custom categories, each of which comprises a set of sites, for your users.

Protocols	Standard setting	Reason for standard setting	Consider changing setting if...
Protocols	Websense standard protocols are provided by default.		You want to create your own custom protocols.

Notification pages	Standard setting	Reason for standard setting	Consider changing setting if...
	Access Denied page displays by default when a policy denies access to a resource. Other standard include error, Cannot connect, HTTP authentication required, and more.	User needs to know why the requested page is not displaying.	You want a custom notification message. You can edit the default messages or create your own from scratch.

Time periods	Standard setting	Reason for standard setting	Consider changing setting if...
Time periods	Afternoon Lunch Morning Working hours	These are the most common time periods our customers use.	You want to set up alternate time periods for your users. You can edit a time period or add a new time period.
Time zones	The time zone you indicated when registering for the service.		Your end users are located in a different time zone or multiple time zones.

Domains	Standard setting	Reason for standard setting	Consider changing setting if...
Policy-level domains	There are no default policy-level domains. When you add one, Include sub-domains is ON. Associate this domain with all policies is OFF.		You have multiple domains and want to apply a separate policy to each domain.
Account-level domains	All domains added on the Connections screen are account-level by default.	We allow you to customize your policies yourself.	You have multiple domains and want to apply a separate policy to each domain. In this case, add a policy-level domain.

Policy settings	Standard setting	Reason for standard setting	Consider changing setting if...
General	Policy name: default Web administrator: email address used to register account Time zone: time zone indicated during registration Time-based access: off		You want to rename your policy to something more meaningful. You are establishing a policy for remote users. Your users are in a different time zone. You want to configure time-based access. You want to apply different authentication methods to different geographical locations.
Connections	By default, all users are treated as remote and must authenticate to use the service.	This gives you the tightest security until you configure your own connections.	If most users are connecting through a single IP address or IP range. In this case, add one or more proxied connections for your policy. Add a non-proxied destination when you want to avoid connecting via our proxy service.
Access Control	By default, all users are treated as remote and must authenticate to use the service.	This gives you the tightest security until you configure your own connections.	You want to monitor user activity without requiring an additional login. You want to use Windows authentication to govern access. (Choose NTLM identification.) You want to authenticate users and you do not have Active Directory.
End Users	By default, end users are expected to self register, but they must be in your domain.		You have a list of users and email addresses that you can upload. In this case bulk register end users to save them time. If you have end users outside of your domain, invite them to register.
File Blocking (only file blocking by extension is supported)	No files are blocked by default.	You must select which file extensions are blocked for categories.	You want to block certain file types for particular categories, users, and groups.

Policy settings	Standard setting	Reason for standard setting	Consider changing setting if...
Web Content & Security	<p>Malware is blocked both inbound and outbound by default.</p> <p>Executables are blocked outbound by default.</p> <p>Real-time classification provided by the Advanced Classification Engine is on if available.</p> <p>Inbound antivirus analysis is enabled for sites with elevated risk profiles.</p> <p>File type analysis is enabled for suspicious and unrecognized files.</p> <p>Real-time classification, antivirus analysis, and advanced detection can be performed only for sites with elevated risk profiles.</p>		<p>Some users require inbound executables.</p> <p>You do not want to block outbound traffic.</p> <p>You want to refine or disable real-time classification.</p> <p>You want to refine or disable antivirus analysis.</p> <p>You want to refine or disable file type analysis.</p>
Web Categories	<p>Default policy blocks access to offensive and adult sites, allows news and entertainment sites, offers no black or white lists.</p>		<p>You want to customize the default policy to align with your company's acceptable use policy.</p>
Protocols	<p>Default policy allows or blocks a protocol based on Websense protocol database default values.</p>		<p>You want to add custom protocols to align with your company's acceptable use policy.</p>
SSL Decryption	<p>Default policy does not decrypt SSL requests for analysis by default.</p>		<p>You want to decrypt SSL requests for all or specific web categories.</p>

A

Checklists for Setting up LDAP in Various Use Cases

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

Whether you are a new or existing customer, you should plan your approach before performing your first synchronization. This section provides checklists for setting up directory synchronization in various use cases. Find yours to determine the best course of action.

- ◆ [New Web and/or email customers](#)
- ◆ [Existing Web and/or email customers](#)
- ◆ [Considerations for existing customers](#)

New Web and/or email customers

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

For new Websense blueSKY and/or customers, see the following:

- ◆ [Synchronizing users/groups with a single Web policy and exceptions, page 129](#)
- ◆ [Synchronizing users/groups with more than one Web policy, and planning to manage Web policy assignment through an LDAP directory, page 130](#)

Synchronizing users/groups with a single Web policy and exceptions

- Plan the portal data structure: users and groups (See [Groups, page 18](#)), policies (See [Defining Web Policies, page 69](#)) and exceptions. (See [Exceptions, page 90](#).)
- Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the proposed portal data structure more closely.
- [To download the client](#); [page 34](#) and install it on the target client machine.
- Configure the Directory Synchronization Client to search the LDAP directory and extract groups and users to a local file (ensure NTLM ID is included). (See

the [Directory Synchronization Client Administrator's Guide](#) for instructions.) Review the results and modify the search as necessary to ensure it returns expected results.

- ❑ In the portal, set up a contact with Directory Synchronization permissions. (See [Set up authentication, page 33](#).) This will be the username/logon used for the Directory Synchronization Client to log onto the portal.
- ❑ Decide whether email will be sent after new users are synchronized from LDAP.
- ❑ Now you are ready! In the portal, enable Directory Synchronization. (See [Configure directory synchronization, page 30](#).)
- ❑ In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide](#).)
- ❑ During a slow period, select **Replace** on the client. Data is synchronized to the portal. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
- ❑ Log onto the portal. Using **Account Settings > End Users**, check that users' policies and groups are as expected. Check the groups list to ensure as expected. (See [View and manage user data, page 34](#).)
- ❑ On the Directory Synchronization page, view Recent Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See [View recent synchronizations, page 36](#).)
- ❑ If you are planning to set up exceptions based on group membership, do this now on the portal. (See [Exceptions, page 90](#).)
- ❑ The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use Restore to undo the synchronization data, and try again. (See [Restore directories, page 37](#).)
- ❑ If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

Synchronizing users/groups with more than one Web policy, and planning to manage Web policy assignment through an LDAP directory

- ❑ Plan the portal data structure: users and groups (See [Groups, page 18](#)), policies (See [Defining Web Policies, page 69](#)) and exceptions. (See [Exceptions, page 90](#).) Create an extra policy or policies as required.
- ❑ Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the proposed portal data structure more closely.
- ❑ [To download the client](#); [page 34](#) and install it on the target client machine.
- ❑ Configure the Directory Synchronization Client to search the LDAP directory and extract groups and users to a local file (ensure NTLM ID is included). (See the [Directory Synchronization Client Administrator's Guide](#) for instructions.)

Review the results and modify the search as necessary to ensure it returns expected results.

- ❑ In the cloud portal, set up a contact with Directory Synchronization permissions. (See [Set up authentication, page 33.](#)) This will be the username/logon used for the Directory Synchronization Client logs into the portal.
- ❑ Decide whether email will be sent after new users are synchronized from LDAP.
- ❑ Now you are ready! In the portal, enable Directory Synchronization. (See [Configure directory synchronization, page 30.](#))
- ❑ In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide.](#))
- ❑ During a slow period, select **Replace** on the client. Data is synchronized to the portal. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
- ❑ Log onto the portal. Using **Account Settings > End Users**, check that users' policies and groups are as expected. Check the groups list to ensure as expected. (See [View and manage user data, page 34.](#))
- ❑ On the Directory Synchronization page, view Recent Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See [View recent synchronizations, page 36.](#))
- ❑ Go to each policy in turn, and set up the group/policy assignments. This moves users to the appropriate policies. (See [Assign a group to a different policy, page 35.](#))
- ❑ Go to the Directory Synchronization configuration page and check that the default policy setting is correct.
- ❑ Return to the **Account Settings > End Users** page and check that users are in the correct policies.
- ❑ If you are planning to set up exceptions based on group membership, do this now on the portal. (See [Exceptions, page 90.](#))
- ❑ The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use Restore to undo the synchronization data, and try again. (See [Restore directories, page 37.](#))
- ❑ If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

Existing Web and/or email customers

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

For existing cloud Web and/or email customers, see the following:

- ◆ [Wanting to manage users/groups from an LDAP directory, page 132](#)

-
- ◆ *Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal, page 133*

Wanting to manage users/groups from an LDAP directory

- ❑ Review the existing portal data structure, specifically the structure of users, groups, and policies. Go to **Account Settings > End Users** and **Account Settings > Groups** to view groups and users. (See [Groups, page 18](#)). Make sure the structure is still as you require. This is a good opportunity to review and amend the structure. Review the exceptions in the policy. (See [Defining Web Policies, page 69](#)) and exceptions. (See [Exceptions, page 90](#).)
- ❑ Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the portal data more closely.
- ❑ Modify portal and/or LDAP data to match each other as closely as possible. You might do this by creating new LDAP groups with the same name and members as the portal groups
- ❑ [To download the client](#); [page 34](#) and install it on the target client machine.
- ❑ Configure the Directory Synchronization Client to search the LDAP directory and extract groups and users to a local file. (See the [Directory Synchronization Client Administrator's Guide](#) for instructions.) Compare the results against the portal data, old CSV files, and/or expectations. Modify the search as necessary to ensure it returns expected results.
- ❑ Decide whether to allow overwriting of groups of the same names. On the portal, set **Overwrite groups** as necessary. (See [Configure directory synchronization](#) for information.) If you allow overwriting, LDAP groups then take over existing groups but retaining their structure in policies and exceptions. If you do not overwrite groups, make sure that all groups being synchronized from LDAP have different names than those in the portal, then change any group-based notification on the portal to the new LDAP names as required.
- ❑ If you have more than one Web policy, go to each policy and assign groups to it (See [Assign a group to a different policy, page 35](#).)
- ❑ Then on the Configure Directory Synchronization screen, assign users to a default policy and for **User policy assignment**, select **Follow group membership**. With this setting, as users are moved to a different LDAP group, their policy assignment changes in step.
- ❑ Decide whether email will be sent after new users are synchronized from LDAP.
- ❑ In the cloud portal, set up a contact with Directory Synchronization permissions. (See [Set up authentication, page 33](#).) This will be the username/logon used for the Directory Synchronization Client logs into the portal.
- ❑ Now you are ready! In the portal, enable Directory Synchronization. (See [Configure directory synchronization, page 30](#).)
- ❑ In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide](#).)

-
- ❑ During a slow period, select **Replace** on the client. Data is synchronized to the portal. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
 - ❑ Log onto the portal. Using **Account Settings > End Users**, check that users' policies and groups are as expected. Check the groups list to ensure as expected. (See [View and manage user data](#), page 34.)
 - ❑ On the Directory Synchronization page, view Recent Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See [View recent synchronizations](#), page 36.)
 - ❑ The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use **Restore** to undo the synchronization data, and try again. (See [Restore directories](#), page 37.)
 - ❑ If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

Wanting to manage users/groups from an LDAP directory but Web policy assignment from the portal

- ❑ Review the existing portal data structure, specifically the structure of users, groups, and policies. Go to **Account Settings > End Users** and **Account Settings > Groups** to view groups and users. (See [Groups](#), page 18). Make sure the structure is still as you require. This is a good opportunity to review and amend the structure.
- ❑ Review the existing LDAP/Active Directory data structure and decide whether restructuring of LDAP is necessary to match the portal data more closely.
- ❑ Modify portal and/or LDAP data to match each other as closely as possible.
- ❑ [To download the client](#): page 34 and install it on the target client machine.
- ❑ Configure the Directory Synchronization Client to search the LDAP directory and extract groups, users, and email addresses to a local file. (See the [Directory Synchronization Client Administrator's Guide](#) for instructions.) Compare the results against the portal data, old CSV files, and/or expectations. Modify the search as necessary to ensure it returns expected results.
- ❑ Decide whether to allow overwriting of groups of the same names. On the portal, set **Overwrite groups** as necessary. (See [Configure directory synchronization](#) for information.) If you allow overwriting, LDAP groups then take over existing groups but retaining their structure in policies and exceptions. If you do not overwrite groups, make sure that all groups being synchronized from LDAP have different names than those in the portal, then change any group-based notification on the portal to the new LDAP names as required.
- ❑ If you have more than one Web policy, go to each policy and assign groups to it (See [Assign a group to a different policy](#), page 35.)
- ❑ Then on the Configure Directory Synchronization screen, assign users to a default policy and for **User policy assignment**, select **Fixed**. With this setting, new Web users are assigned to the Web policy when first synchronized into the service. After that you must manage all movement of users between policies on the portal using the Manage Users page. (Group membership is ignored.)

-
- ❑ Decide whether email will be sent after new users are synchronized from LDAP.
 - ❑ In the cloud portal, set up a contact with Directory Synchronization permissions. (See [Set up authentication, page 33.](#)) This will be the username/logon used for the Directory Synchronization Client logs into the portal.
 - ❑ Now you are ready! In the portal, enable Directory Synchronization. (See [Configure directory synchronization, page 30.](#))
 - ❑ In the Directory Synchronization Client, set up portal settings in the configuration established above, changing the output type to portal (not file) and using the contact with Directory Synchronization permissions created above. (See the [Directory Synchronization Client Administrator's Guide.](#))
 - ❑ During a slow period, select **Replace** on the client. Data is synchronized to the portal. Note the number of additions. This is visible in the Synchronization page and also from the notification email messages.
 - ❑ Log onto the portal. Using **Account Settings > End Users**, check that users' policies and groups are as expected. Check the groups list to ensure as expected. (See [View and manage user data, page 34.](#))
 - ❑ On the Directory Synchronization page, view Recent Synchronizations and compare the totals of additions against those noted in the Directory Synchronization Client. They should match. (See [View recent synchronizations, page 36.](#))
 - ❑ The system is now live. If you are unhappy with the user/groups data you have synchronized then you can use Restore to undo the synchronization data, and try again. (See [Restore directories, page 37.](#))
 - ❑ If everything appears to be working, set up a schedule time in the Directory Synchronization Client for the background task to run. Close the client tool.

Considerations for existing customers

Websense blueSKY Security Gateway Help | Cloud Web Security Solutions

If you have already set up users, groups, passwords, policies, and exceptions in the cloud portal and you want to switch to LDAP synchronization, consider the following:

- ◆ You can minimize the impact by carefully matching your LDAP group names and membership to the existing setup. Matching LDAP group names and membership to those already in the cloud-based service allows existing policy selections and settings to be maintained, as well as existing usernames/passwords where applicable.
- ◆ You are responsible for avoiding ambiguous configurations, for example, users belonging to multiple groups which are assigned to different policies. It is up to you to set up groups in the LDAP directories in such a way that ambiguities don't occur. (When there are ambiguities, the service selects the closest group-to-policy assignment for each individual user, taking the first group in alphabetical order where there are multiple assignments at the same hierarchical level.)

-
- ◆ Existing users can retain their passwords and whether you manage users through the portal, LDAP synchronization, or both is completely transparent to them.



Index

A

- access control, 75
- Access control tab, 75
- Account Settings, 11
- Account Summary report, 109
- accounts
 - configuring, 21
 - unlocking, 17
- actions, 88
 - Quota, 89
- Active Directory, 23
- Add a domain, 82
- adding
 - Always Analyze or Never Analyze list entries, 104
- adding a custom protocol, 43
- adding groups, 19
- Advanced Classification Engine (ACE), 99
- Always Analyze list
 - adding sites, 104
 - deleting entries, 104
- analysis applications, 102
- analysis files, 102
- analysis options
 - categorizing content, 101
 - saving changes, 101
- Analyze links embedded in Web content, 101
- antivirus analysis options, 102
- applets
 - quota time, 90
- appliance alerts, 67
- appliance management
 - adding an appliance, 62
 - authentication, 63
 - certificates, 63
 - changing the appliance password, 65
 - deleting an appliance, 67
 - properties and statistics, 66
 - registering an appliance, 65

- trusted network sources, 63
- appliance upgrade, 66
- appliance version history, 66
- application analysis, 102
- assigning policies to groups, 83
- audit trail
 - configuration, 123
- Authenticate users, 76
- authentication
 - LDAP, 33
 - scenarios, 75
- authentication settings, 75

B

- block pages
 - Continue button, 89
 - Use Quota Time button, 89
- Browse Time reports, 116
- bulk registering end users, 81
- bypass
 - authentication and certificate verification, 56

C

- categories
 - advanced malware command and control, 93
 - advanced malware payloads, 93
 - custom, 41
 - defined, 93
 - mobile malware, 93
 - unauthorized mobile marketplaces, 93
- categorized reports, 111
- categorizing content, 101
- category list, Web, 92
- changing passwords, 17
- changing the appliance password, 65
- Cloud Service reports, 114
- configuration audit trail, 123
- configuring accounts, 21
- Confirm, 89

- Connections tab
 - Web, 74
- contact information, 12
- Contacts, 12
- content
 - categorization, 101
 - threat analysis, 101
- content analysis options, 101
- Continue button, 89
- cookies, use of, 1, 2
- custom categories, 41
 - importing, 42
- custom protocols, 43
 - adding, 43
 - deleting, 43
 - editing, 44
 - identifiers, 43
 - searching, 43
- D**
- Dashboard, 5
- deleting a custom protocol, 43
- deleting an appliance, 67
- destinations, non-proxied, 75
- directory synchronization, 13, 19, 30, 80, 83
 - modifying groups, 83
 - reporting, 107, 114
- Directory Synchronization Client, 33
- displaying a pre-login welcome page, 76
- disposition order, 92
- dispositions
 - web filter, 88
- Do not block, 89
- domains
 - account-level, 53
 - editing, 54
 - policy-level, 52
- download Directory Synchronization Client, 34
- dynamic content
 - categorizing, 101
- E**
- editing a custom protocol, 44
- Enable LDAP, 30

- enabling an appliance, 62
- end user search, 11
- end users, 20
 - bulk registering, 81
 - searching, 20
- End users tab, 79
- end-user registration pages, editing, 85
- end-user self registration, 82
- exceptions, 90
- expiration limit, password, 16

F

- failures, synchronization, 38
- file analysis
 - file extensions, 103
 - options, 102
- File Blocking tab, 97
- file extensions
 - filtering by, 97
 - for analysis, 103
- filtering
 - search images, 73
- Force full resync, 38
- forgotten passwords, 18
- full traffic logging, 55

G

- General tab
 - Web, 70
- groups
 - adding, 19
 - downloading or uploading, 19

H

- HTML tag list, Web notifications, 48

I

- idle timeout, 2
- importing custom categories, 42

L

- landing page, 2
- language support, 50
- LDAP
 - authentication, 33

- basic steps, 29
- defined, 24
- directories, 23
- how Cloud Security works with, 24
- restoring directories, 36
- licenses, 7
 - accepting, 8
 - current, 7
 - pending, 7
 - previous, 7
- limiting access time, 90
- locked accounts, 16
- login process, 1
- logs
 - full Web traffic, 55
- M**
- manage user data, 20
- Manage Users, 13
- managing an appliance
 - adding an appliance, 62
 - changing the appliance password, 65
 - deleting an appliance, 67
 - properties and statistics, 66
 - registering an appliance, 65
 - version history, 66
 - viewing alerts, 67
- managing registered users, 85
- Master Database
 - categories, 93
- master user, 13
- Modify Configuration, 13
- monitoring email dispatch, 82
- N**
- Never Analyze list
 - adding sites, 104
 - deleting entries, 104
- notification pages, 44
- NTLM
 - credentials, 78
 - identification, 77
 - identity, 77
 - limitations, 78
 - registration page, 77
 - security implications, 78
- NTLM IDs, synchronizing, 80
- O**
- Overwrite groups, 31
- P**
- passwords
 - changing, 17
 - expiration, 14
 - forgotten, 18
 - settings, 14
 - strength, 15
- permissions
 - for domain configuration, 54
- policies
 - Web, 69
- policy-specific PAC file address, 71
- portal interface
 - banner, 3
- portal security, 1
- privileges, user, 13
- protocol identifier, 43
- protocols, 43
- proxied connections, 74
- Q**
- Quota, 89
- quota time, 90
 - applets, 90
 - sessions, 90
- R**
- real-time content classification, 99
- real-time options
 - file analysis, 102
- real-time security classification, 100
- registering an appliance, 65
- registering users by invitation, 80
- registration, directory synchronization, 80
- removing
 - Always Analyze or Never Analyze list entries, 104
- reporting, 107

- Cloud Service reports, 114
 - directory synchronization, 107, 114
- reporting periods, 108
- reports
 - browse time, 116
 - categorized, 111
 - drilling down, 112
 - list of, 116
 - results, 112
 - saving, 112
 - scheduling, 113
- restore LDAP directories, 36
- rules
 - policy association during end user registration, 85

S

- saving reports, 112
- scheduling reports, 113
- search filtering, 73
- searching custom protocols, 43
- security threats
 - scanning for, 101
- Setup
 - Web, 41
- surfing time periods, 51
- synchronization failures, 38
- Synchronization History Log, 115
- Synchronization Time Summary, 115

T

- threat analysis, 101

- threats
 - in files, 102
 - in Web pages, 101
- time periods, configuring Web, 51
- time zones
 - policy, 71
 - proxied connections, 74
 - time periods, 51
- time-based access control, 72
- time-based Internet access, 90
- timeout, 2
- toolbar, 3
- troubleshooting, sync failures, 38

U

- unlocking user accounts, 17
- use quota time, 90
 - block page button, 89
- user lockout, 16

V

- View All Reports, 13
- View Configuration, 14
- View Configuration Audit Trail, 14
- viewing appliance alerts, 67

W

- Web administrator, 71
- Web Categories tab, 87
- Web Content & Security tab, 99
- welcome page, 76