websense

TRITON - Data Security Help

Websense® Data Security

v7.5

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2010

Printed in the United States and Ireland

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

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.

Contents

Part I: Getting Started

Part II: Securing Your Company's Data

Part III: Administering the System

Part IV: Appendices

Part I

Getting Started

1 Overview

Websense® Data Security protects organizations from information leaks and data loss both at the perimeter and inside the organization.

Websense Data Security can operate alone in the network, or be paired with Websense Web and email security solutions (on-premises or in the cloud), to provide a well-rounded Essential Information Protection solution for your organization.

Websense Data Security protects organizations from data loss by:

- Discovering the location of sensitive data inside the network
- Monitoring data as it travels inside or outside the organization
- Protecting data while it is being manipulated in office applications, with policy-based controls that align with business processes

The 2 main components of Websense Data Security are:

- The Data Security Management Server
- The Data Security Protector

The Data Security Management Server is a Windows 2003-based machine where you install the Websense Data Security software. This machine provides the core information loss technology, capturing fingerprints, applying policies, and storing incident forensics. You can install multiple Data Security servers, sharing the analysis load, but one must be the primary, management server.

The protector is a Linux-based machine that intercepts and analyzes traffic on a variety of channels, such as email, HTTP, FTP, and chat. It is an essential component of Websense Data Security providing monitoring and blocking capabilities to prevent data loss and leaks of sensitive information. Using PreciseID technology, the protector can accurately monitor sensitive information in transit on any port.

In addition, Websense Data Security can utilize a variety of agents to intercept data on Exchange servers, print servers, and more. Endpoints that are deployed on users' computers (PCs, laptop, etc.) enable administrators to analyze content within a user's working environment and block or monitor policy breaches as defined by the endpoint profiles.

What can I protect?

Related topics:

- *Sources and destinations*, page 103
- *Classifying Content*, page 69
- *Defining Resources*, page 101
- *Remediation*, page 112

Websense Data Security lets you control or monitor the flow of data throughout your organization. You can define:

- Who can move and receive data
- What data can and cannot be moved
- Where the data can be sent
- How the data can be sent
- What action to take in case of a policy breach

Websense Data Security secures:

- **Network printers -** You can monitor or prevent sensitive data from being printed on any printer in your network.
- **Endpoint applications -** You can monitor or prevent sensitive data from being copied and pasted from one application to another on endpoint clients. This is desirable, because endpoint clients are often disconnected from the corporate network and can pose a security risk.
- **Endpoint removable media -** You can monitor or prevent sensitive information from being written to a removable device such as a USB flash drive, CD/DVD, or external hard disk.
- **Endpoint LANs -** Users commonly take their laptops home and then copy data through a LAN connection to a network drive/share on another computer.
  - You can specify a list of IPs, hostnames or IP networks of computers that are allowed as a source or destination for LAN copy.
  - You can intercept data from an endpoint client.
  - You can set a different behavior according to the endpoint type (laptop/other) and location (connected/not connected).

  Note that Endpoint LAN control is applicable to Microsoft sharing only.
- **Email systems -** You can monitor or prevent sensitive information from being emailed in or outside of your domain.
- **Web channels**
  - **FTP -** You can monitor or prevent sensitive information from being uploaded to file transfer protocol (FTP) sites.

- **Chat -** You can monitor sensitive information going out via instant messenger applications such as Yahoo! Messenger.
- **Plain text -**You can monitor or prevent sensitive information from being sent via plain text (unformatted textual content).
- **HTTP/HTTPS -** You can monitor or prevent sensitive information from being posted to a Web site, blog, or forum via HTTP. You can also prevent users from downloading sensitive data from the Web.
- **Endpoint HTTP/HTTPS -** You can monitor or protect endpoint devices such as laptops from posting or downloading sensitive data over the Web.

By such comprehensive monitoring of these channels, you can prevent data from leaving your organization by the most common means.

PreciseID fingerprinting

Related topics:

- *PreciseID Fingerprinting - files & directories*, page 84
- *PreciseID Fingerprinting - database records*, page 89
- *PreciseID Natural Language Processing (NLP)*, page 82
- *Classifying Content*, page 69

One of the ways that you can classify data in your organization is by “fingerprinting” it using the Websense patented PreciseID™ technology. (Other ways include identifying key phrases, regular expression patterns, dictionaries, or file types. See *Classifying Content*, page 69.)

The power of PreciseID techniques is its ability to detect sensitive information despite manipulation, reformatting, or other modification. Fingerprints enable the protection of whole or partial documents, antecedents, and derivative versions of the protected information, as well as snippets of the protected information whether cut and pasted or retyped.

PreciseID technology can fingerprint 2 types of data: structured and unstructured.

- Structured fingerprinting defines what tables and what data inside the table should be fingerprinted. (To set this up, select **Main** > **Policy Management** > **Content Classifiers** > **PreciseID Fingerprinting - Database Records**.)
- Unstructured fingerprinting defines files and folders that should be fingerprinted. (To set this up, select **PreciseID Fingerprinting - Files & Directories**.)

PreciseID classifiers not only define what to fingerprint, but when and how often to run the fingerprinting scan. That way, if files or data change after fingerprinting, Data Security stays up to date.

At scan time, PreciseID technology examines the content of documents or raw data and extracts a set of mathematical descriptors or “information fingerprints.” These fingerprints are compact and describe the underlying content. By assigning unique identities to each information asset, PreciseID technology can track information in motion with great precision. Original content cannot be recreated or reverse engineered from the PreciseID information fingerprint.

PreciseID supports real-time hash validation for data identification and integrity.

You can fingerprint data in all common languages. Websense has fine-tuned fingerprinting for English, Spanish, German, Russian, Hebrew, and Japanese.

Policy database and engine

Related topics:

- *Balancing the load*, page 278
- *Configuring the policy engine*, page 254

There is a policy database and a policy engine on all Websense Data Security servers and the protector. The policy database is a repository for all of the policies you create. For optimal performance, it is stored locally on each server, as is the fingerprint database. The policy database is “pushed” during the deploy operation, while fingerprints are distributed automatically as they are generated.

The policy engine is responsible for parsing your data and using analytics to compare it to the rules in your policies. If you are combining Websense Web and Data Security solutions, the policy engine resides on the Websense Content Gateway as well. This allows the 2 systems to interoperate seamlessly to secure your enterprise. A policy engine also resides on endpoints, but with only unstructured fingerprints.

Managing Websense Data Security

Related topics:

- *Navigating the System*, page 7

The interface that you use to manage Websense Data Security is called the **TRITON™ Unified Security Center**. TRITON has modules for both Web security and data security. TRITON is a Web-based user interface that enables you to perform basic setup, system maintenance, policy creation, reporting, and incident management for both modules in the same location.

✓ **Note**

TRITON Unified Security Center supports Internet Explorer 7 and 8 and Firefox 3.0.x - 3.5.x. If you have another browser version, unexpected behavior may result.

To access **TRITON - Data Security**, click the Websense TRITON Data Security shortcut placed on the desktop during installation or select **Websense TRITON Data Security** from your **Start** menu.

TRITON - Data Security consolidates all aspects of Websense Data Security setup and configuration, incident management, system status reports, and role-based administration.

For more information on using the TRITON - Data Security interface, see *Navigating the System*, page 7.

Web Security Gateway Anywhere mode

Websense Data Security works seamlessly with Websense Web Security and Websense Web Security Gateway. You can purchase full subscriptions for these products to make use of their complete capabilities.

If you have Websense Web Security Gateway Anywhere, data loss is prevented on Web channels only and you are not required to purchase a separate Data Security subscription or a protector appliance.

The Web channels covered by Web Security Gateway Anywhere include HTTP, HTTPS, FTP, and FTP-over-HTTP. This allows you to prevent posts to Web sites, blogs, and forums as well as FTP sites.

✓ **Note**

If you have Websense Web Security Gateway Anywhere, you won’t see all the options that are presented in this Help system. If you require access to other options and channels that you see here, talk to your Websense account representative about purchasing a full Websense Data Security subscription.

2 Navigating the System

In this section, you will learn how to navigate the TRITON - Data Security interface. It covers:

- *Logging on*
- *Collapsible navigation and content panes*
- *Today page*
- *Toolbar*
- *Icons*
- *Breadcrumbs*
- *Check boxes*
- *Pagination*
- *Reviewing and deploying changes*

Logging on

There are 3 ways to access TRITON - Data Security:

- Click the Websense TRITON - Data Security shortcut placed on the desktop during installation.
- Select **Start** > **Programs** > **Websense** > **Websense TRITON - Data Security** from your Windows **Start** menu.
- Open a browser window, and enter the following URL into the address field:

  ```
  https://<IP_or_hostname>:8443/dlp/pages/mainFrame.jsf
  ```

  where <IP_or_hostname> is the IP address or host name of the Data Security Management Server.

> ✓ **Note**
>
> The host name must not contain underscore characters.

Initially, your user name and password are both “admin” (case-sensitive). Enter these credentials and click **Log On**.

In the Change Password screen, type the old password, “admin” then enter a new password and retype it for confirmation. Click **Save & Log On**.

✓ **Note**

A maximum of 20 users can be signed in simultaneously, each in a separate browser instance. Opening more than one session of TRITON - Data Security in the same browser results in unexpected behavior.

Troubleshooting log on

If you are unable to connect to TRITON - Data Security on the default port, refer to the **dlp-all.log** file on the Data Security Management Server (located by default in the C:\Program Files\Websense\data security\tomcat\logs\dlp directory) to verify the port.

If you are using the correct port, and are still unable to connect to TRITON - Data Security from a remote machine, make sure that your firewall allows communication on that port.

Security certificate alerts

An SSL connection is used for secure, browser-based communication with TRITON - Data Security. This connection uses a security certificate issued by Websense, Inc. Because the supported browsers do not recognize Websense, Inc., as a known Certificate Authority, a certificate error is displayed the first time you launch TRITON - Data Security from a new browser. To avoid seeing this error, you can install or permanently accept the certificate within the browser.

1. Click the link on the log on page for instructions on installing the certificate.
2. When asked “Would you like to install the certificate on this server?”, click **Yes**. (Select **Don’t show this alert on the logon screen again** to permanently remove the note from the logon screen.)
3. If a yellow bar appears at the top of the resulting browser window, click it and download the required ActiveX control.
4. Click **Install** to install the Websense certificate.

Once the security certificate has been accepted, the TRITON - Data Security logon page is displayed in the browser window.

Windows 7 considerations

If you are using the Windows 7 operating system, you may need run the browser as administrator for it to allow ActiveX controls.

1. Right-click the browser application and select **Run as administrator**.
2. Log on to TRITON - Data Security and accept the security certificate as described above.

Adobe Flash Player

Adobe Flash Player v8 or beyond is required for the Data Security Today and System Health dashboards. All the other functions of the manager interface can operate without Flash. If you do not already have Flash Player, you are prompted to install it when you log on. Click the link that is supplied and download Flash Player from the Adobe download center.

Time outs

A TRITON - Data Security session ends 30 minutes after the last action taken in the user interface (clicking from page to page, entering information, caching changes, or saving changes).

If no activity has taken place in TRITON - Data Security during this time, you are logged out, even if you are working in other modules of the TRITON security center.

If you have multiple *tabs* in the same browser displaying TRITON - Data Security and you are working in one of the tabs, the others do not expire.

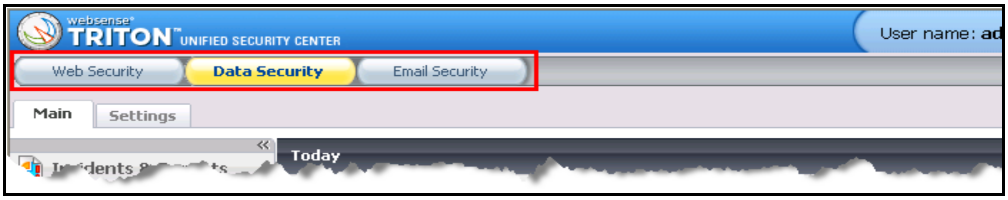
If you have multiple *windows* displaying TRITON - Data Security and you are working in one of the windows, the time out behavior depends on the browser type:

- In Firefox and Internet Explorer v8, the other windows do not expire
- In Internet Explorer v7, the other windows expire

> ✓ **Note**
>
> If you have multiple TRITON - Data Security instances open, whether in browser tabs or windows, changes made in one are reflected in the others once you refresh the screen.

The TRITON module tray

The TRITON module tray indicates which module is active.



When you log onto TRITON - Data Security, the Data Security module is active and the Data Security button in the module tray is yellow. When you're in TRITON - Web Security, the Web Security button is yellow, and the Data Security button is grey.

If you have a subscription to Websense Web Security, Websense Web Security Gateway, or Websense Web Security Gateway Anywhere, you can enable the buttons in the module tray so that administrators can easily switch between TRITON - Web Security and TRITON - Data Security. (You must have administrator accounts with the same user names and passwords in both managers for this to work.) See *Linking data and Web security*, page 226 for instructions on configuring this option.

✓ **Note**

Once you have opened both management consoles in the TRITON security center, use the operating system task bar to switch between the two.

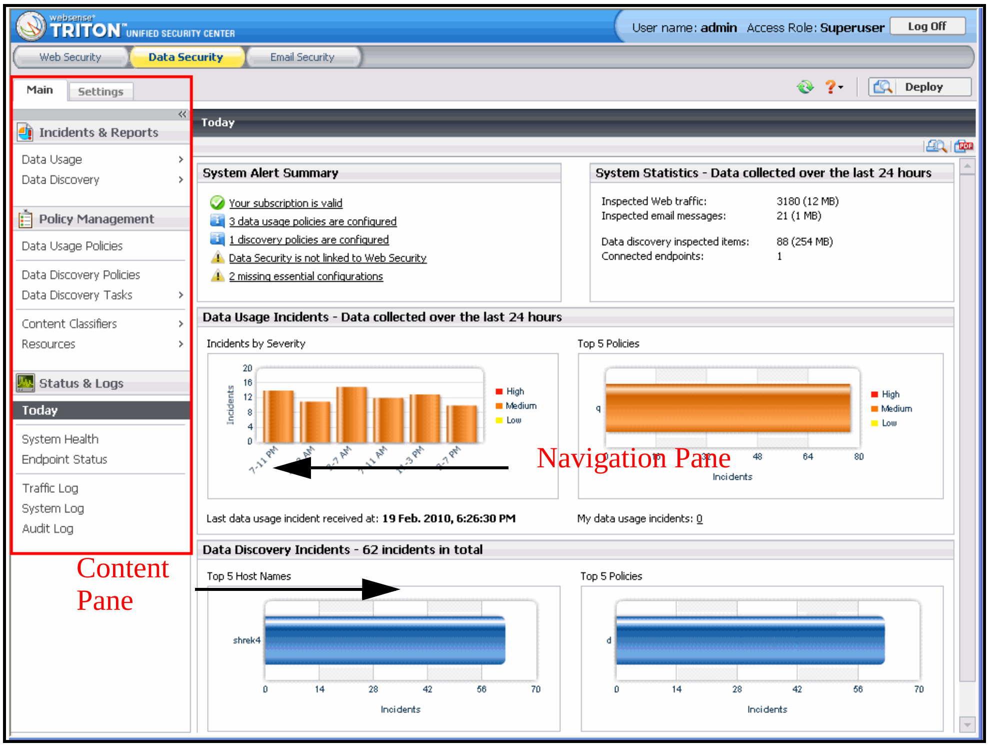
Until you configure linking, clicking the Web Security button opens a Web page describing the benefits of Websense Web security solutions.The Email Security button displays a similar Web page.

Collapsible navigation and content panes

Related topics:

- *Main tab*, page 12
- *Settings tab*, page 13

The left pane of the TRITON Unified Security Center is known as the **navigation** pane. The navigation pane is organized with tabs and buttons, some of which offer a menu of options. The right pane is known as the **content** pane. The content in this pane varies according to the selection in the navigation pane.



Your subscription is valid
3 data usage policies are configured
1 discovery policies are configured
Data Security is not linked to Web Security
2 missing essential configurations

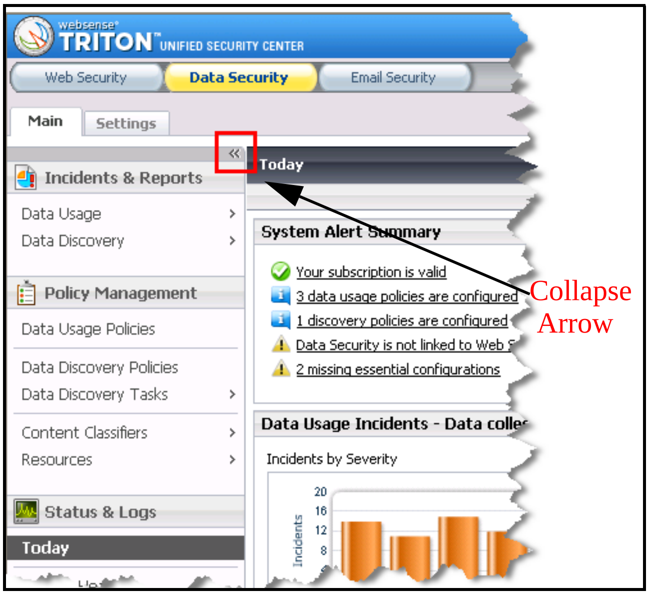
Inspected Web traffic:	3180 (12 MB)
Inspected email messages:	21 (1 MB)
Data discovery inspected items:	88 (254 MB)
Connected endpoints:	1

Last data usage incident received at: 19 Feb. 2010, 6:26:30 PM

My data usage incidents: 0

The navigation pane is collapsible to enable larger working space and a wider display area for all TRITON pages. In TRITON - Data Security, this is especially useful for the Data Usage and Data Discovery reports.

To collapse the navigation pane, click the arrows in the upper-right corner of the pane. To expand it, click the arrows again. You can do this on any page in the TRITON security center.



Your subscription is valid
3 data usage policies are configured
1 discovery policies are configured
Data Security is not linked to Web S
2 missing essential configurations

There are 2 tabs on the navigation pane: Main and Settings. In TRITON - Data Security:

- The *Main tab* is where you create and fine-tune policies, perform discovery, manage incidents, and view system status and logs.
- The *Settings tab* is where you administer the system. Here, you can perform system maintenance; configure endpoint deployment; and configure settings, modules, and roles.

> ✓ **Note**
>
> If you have Websense Web Security Gateway Anywhere, your tabs look slightly different. That's because not all of the options apply to you, such as discovery and endpoint.

Main tab

Related topics:

- *Viewing Incidents and Reports*, page 159
- *Creating a custom policy*, page 49
- *Performing Discovery*, page 123
- *Scheduling Data Discovery Tasks*, page 135
- *Classifying Content*, page 69
- *Defining Resources*, page 101
- *Viewing Status and Logs*, page 197

*Not included with Websense Web Security Gateway Anywhere.

Incidents & Reports

- **Data Usage:** View and manage data usage incidents relevant to the active administrator. You can assign incidents to other administrators and view consolidated reports on incidents and information leaks. This gives you a complete picture of what's going on inside your network. You can also schedule reporting tasks.
- **Data Discovery*:** View information about incidents that were discovered through data discovery. Using this screen, you can assign, view, and monitor data discovery incidents.

Policy Management

- **Data Usage Policies:** Create or manage a network policy or endpoint policy. You can create policies from scratch or by using a predefined regulatory template.
- **Data Discovery Policies*:** Create or manage a data discovery policy. You can create policies from scratch or using a predefined regulatory template.

- **Data Discovery Tasks*:** Schedule data discovery tasks.
- **Content Classifiers***:* Describe the data to be governed. You can classify data by file properties, key phrases, dictionaries, natural-language patterns (NLP), a database record fingerprint, a directory (including SharePoint) fingerprint, and/or a file fingerprint.
- **Resources:** Define the source and destination of the data you want to protect, the endpoint device or application that may be in use, and the remediation or action to take when a violation is discovered (such as block or notify).

Status & Logs

- **Today:** The **Today** page appears first when you log on to TRITON - Data Security. It provides an at-a-glance dashboard of the enterprise data loss prevention status.

  For more information about the Today page, see *Today page*, page 14.
- **System Health:** This enables you to monitor Websense Data Security performance. See *Monitoring system health*, page 200.
- **Endpoint Status***: On this page you can view a list of data endpoints that are registered with the Data Security Management Server, including information regarding an endpoint's data discovery, profile and policy, and the host's system summary. See *Viewing endpoint status*, page 202.
- **Traffic Log**: This enables you to see details of the traffic being monitored by Websense Data Security. See *Traffic log*, page 204.
- **System Log:** Here you can view a list of the events sent from system components, such as the Data Security servers, protectors, and policy engines. See *System log*, page 205.
- **Audit Log:** This page displays a list of actions that administrators have performed in the system. See *Audit log*, page 206.

Settings tab

Related topics:

- *Configuring System Settings*, page 209
- *Configuring Authorization*, page 231
- *Archiving Incidents*, page 239
- *Managing System Modules*, page 243
- *Configuring Endpoint Deployment*, page 281
- *Main tab*, page 12

*Not included with Websense Web Security Gateway Anywhere.

Configuration

- **System:** Configure basic system settings for incidents and forensics, user directories, mail gateways, Websense product integration, and more.
- **Authorization:** Set up and manage TRITON - Data Security system administrators, assign access roles, and change your own password.
- **Archive:** Archive partitions for incident storage.

Deployment

- **System Modules:** Manage system components such as Data Security servers, fingerprint repositories, policy engines, and agents.
- **Endpoint*:** Configure endpoint profiles.

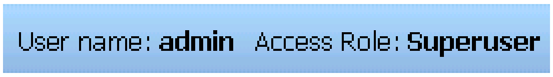
Today page

When you log onto TRITON - Data Security, the Today page displays. This page includes a comprehensive view of data usage incidents that occurred in the last 24 hours, and the total number of data discovery incidents.

From the Today page, you can see any system alerts and act on them quickly and easily. You can also view incidents by host names and policy categories so you know where your greatest risks lie.

For details about the Today page and its contents, see *Viewing the Today page*, page 198.

Toolbar


User name: **admin** Access Role: **Superuser**

The top banner displays the user name and access role of the person who is logged into the system. The user's access role affects the screens and incidents that he or she can view.

Click this button to log off from TRITON - Data Security.

The **Refresh** button updates the data on the screen.

The **Help** button (the question mark icon) is your access to information whether you are learning how to use the system or troubleshooting it.

You have several options in the Help's drop-down menu:

- **Explain this page:** Context-sensitive help about the active TRITON - Data Security screen. To access the entire Help system from the context help page, click the **Browse** button in the upper-left corner of the help page.
- **Help Contents:** The complete online Help system for Websense Data Security.
- **Support Portal:** Quick access to the Websense Customer Support portal and Knowledge Base.
- **About TRITON - Data Security:** Version information about the software you've licensed.

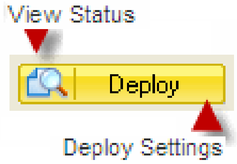
> **Tip**
>
> In addition to these Help features, many screens offer an information icon: ⓘ
>
> This is another tool for user assistance. The ⓘ icon displays vital information about its related field.

In Websense Data Security, your policy and configuration changes are saved as soon as you make them and click **OK**, but they are localized to the Data Security Management Server.

To deploy changes across your network, you must click the **Deploy** button on the TRITON banner. (See *Reviewing and deploying changes*, page 22.)

The **Deploy** button deploys your policy changes across all network components—the protector, agents, gateways, endpoint hosts, etc. This includes changes to policies, rules, exceptions, resources, content classifiers, and tasks.

If you have changes waiting to be deployed, the **Deploy** button is highlighted yellow to indicate the deployment is required.



Click the left button (the magnifying glass icon) to view the status of the last deployment. Click the right button to deploy the settings you configured.

If no changes are awaiting deployment, the **Deploy** button is white, but you can still view deployment status.

If you are not allowed to deploy or see the last status, these buttons are greyed out.

In TRITON - Web Security, the **Save All** button performs a similar function.

Note

Deploy is not the same as **Enabled**. When you create Websense Data Security rules, exceptions, and policies, you mark them as Enabled or Disabled. You can deploy them in either state. You might deploy a policy with all its rules enabled, and later want to disable a rule because of false positives. Or you might disable the entire policy temporarily.

Icons

The following icons are used throughout the TRITON - Data Security interface:

Icon	Description
System Modules	
	Data Security Management Server
	Data Security Server
	Protector

Icon	Description
	Content Gateway
✉	SMTP agent
🌐	ISA agent
🖨	Printer agent
	Exchange agent
✉	WES agent
	PreciseID fingerprint repository
💻	Endpoint server
	Crawler
	Forensics repository
	Policy engine
iCAP	ICAP server
Deployment Status	
✎	Modified
	Disabled

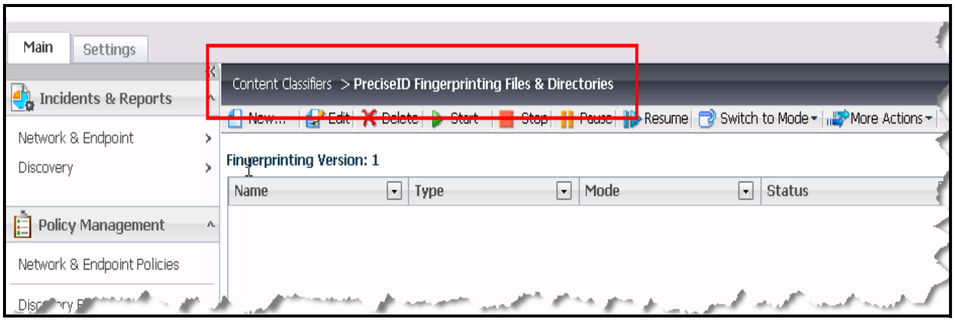
Icon	Description
	Forced Bypass
Severity	
H	High
M	Medium
L	Low
Incident Status Flags	
🚩	New
⚑	In Process
⚐	Closed
Endpoint Operations	
🖨	Print
⧉	Cut/copy
📋	Paste
➡	File access
⬇	Download
📷	Screen capture

Icon	Description
Channels	
	HTTP
	Endpoint
	Exchange
	FTP
☺	IM
🖨	Printer
✉	SMTP
iCAP	ICAP
🌐	Web
Details report	
	Escalate
	Hide preview
	Show preview
16	Add scheduled task - accesses the Task Scheduler screen
🔍	Print preview - Current, selected, or all filtered incidents

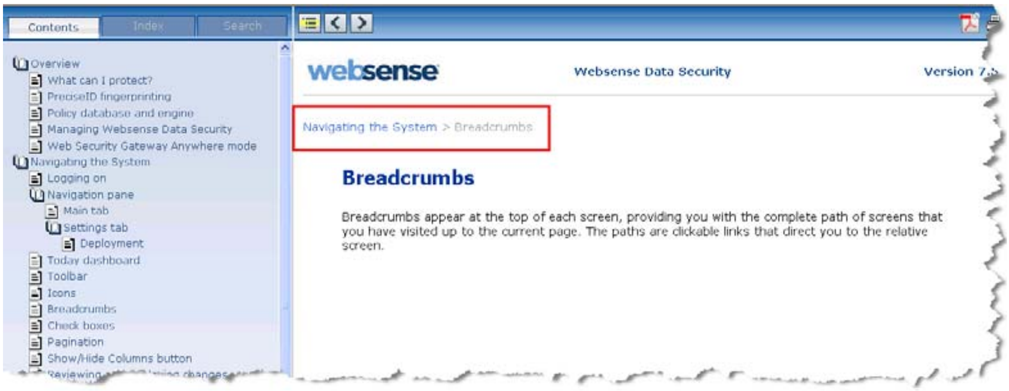
Icon	Description
Incidents & Reports	
▦	Details report
◔	Summary report
Print and Export	
PDF	Export as PDF
CSV	Export as CSV
🔍	Print Preview
System-wide	
✖	When a user modification or update to the system fails, the Error icon is displayed at the top of the screen with an explanation of the failure.
✓	When a user modification or update to the system succeeds, the Success icon is displayed at the top of the screen with a description of what has been done.
ℹ	The Information icon provides added details upon click.
🗒	The Note icon is displayed when extra information is supplied that is pertinent to the configuration.

Breadcrumbs

Breadcrumbs appear at the top of each screen, providing you with the complete path of screens that you have visited up to the current page. The paths are clickable links that direct you to the relative screen.



The Help system also includes breadcrumbs.

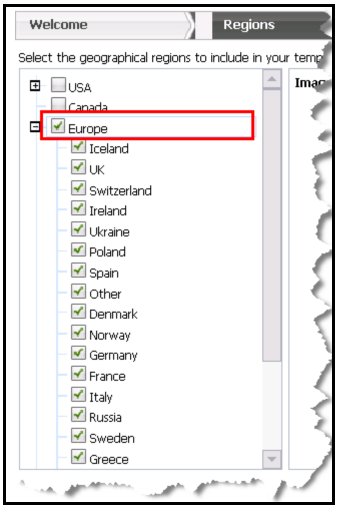


Breadcrumbs

Breadcrumbs appear at the top of each screen, providing you with the complete path of screens that you have visited up to the current page. The paths are clickable links that direct you to the relative screen.

Check boxes

Most check boxes used in the TRITON - Data Security interface function in a hierarchical manner. In tables, the title check box enables you to select or deselect all the check boxes below it. In forms, clicking a check box allows you to access the check boxes below it and then activate them as necessary. Disabling the highest-level check box disables lower-level check boxes as well.

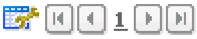


Select the geographical regions to include in your temp

- ⊞ □ USA
- □ Canada
- ⊟ ☑ Europe
  - ☑ Iceland
  - ☑ UK
  - ☑ Switzerland
  - ☑ Ireland
  - ☑ Ukraine
  - ☑ Poland
  - ☑ Spain
  - ☑ Other
  - ☑ Denmark
  - ☑ Norway
  - ☑ Germany
  - ☑ France
  - ☑ Italy
  - ☑ Russia
  - ☑ Sweden
  - ☑ Greece

Pagination

In tables where there is more than one page of data (more than 50 items), the pagination control enables you to move from one page to another.



The **Next** and **Previous** buttons move to the next or previous pages, while the **First** button moves to the first page and the **Last** button accesses the final page.

Reviewing and deploying changes

In Websense Data Security, your policy and configuration changes are saved as soon as you make them, but they are not deployed across your network until you click the **Deploy** button on the TRITON banner.

If you have changes waiting to be deployed, the **Deploy** button turns yellow and flashes occasionally to indicate the deployment is required. If no changes are awaiting deployment, the **Deploy** button is white. If the user has no permission to deploy or to see the last deployment status, the button is greyed out.

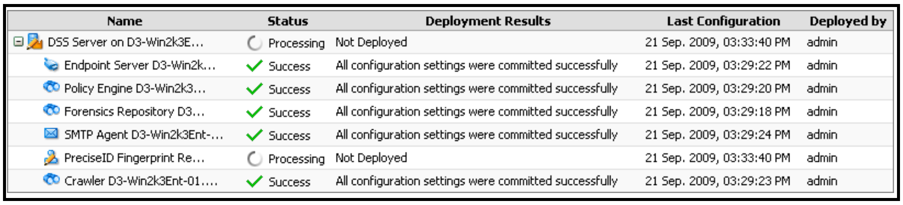
Before you click **Deploy**, be sure to review your configuration changes.

When you click **Deploy**, a confirmation message appears:

```
You are about to deploy the current settings. Click OK to
continue.
```

Click **OK** to deploy the changes across your network.

You will see a table indicating the dynamic status of the components being deployed.



Name	Status	Deployment Results	Last Configuration	Deployed by
⊟ DSS Server on D3-Win2k3E...	Processing	Not Deployed	21 Sep. 2009, 03:33:40 PM	admin
Endpoint Server D3-Win2k...	✓ Success	All configuration settings were committed successfully	21 Sep. 2009, 03:29:22 PM	admin
Policy Engine D3-Win2k3...	✓ Success	All configuration settings were committed successfully	21 Sep. 2009, 03:29:20 PM	admin
Forensics Repository D3...	✓ Success	All configuration settings were committed successfully	21 Sep. 2009, 03:29:18 PM	admin
SMTP Agent D3-Win2k3Ent-...	✓ Success	All configuration settings were committed successfully	21 Sep. 2009, 03:29:24 PM	admin
PreciseID Fingerprint Re...	Processing	Not Deployed	21 Sep. 2009, 03:33:40 PM	admin
Crawler D3-Win2k3Ent-01....	✓ Success	All configuration settings were committed successfully	21 Sep. 2009, 03:29:23 PM	admin

Deploying changes can take time, and if a component is down or disconnected from the network, deployment can fail. If Websense Data Security encounters problems, you’ll see a message indicating deployment failure in the table.

While your changes are being deployed across your network, you can see the status column updates for each module from **Processing** to either **Success** or **Failed**.

See *Troubleshooting* for tips on how to solve failed deployments.

Note

When deploying settings to the protector, active instant messenger (IM) sessions are no longer monitored. Every IM session that is opened after the deploy is monitored; however, existing connections are not be monitored after the deploy.

If you have deployed a protector is in inline mode, when you deploy changes to network settings, users lose an Internet connection for approximately 5 seconds.

3 Initial Setup

Related topics:

- *Entering your subscription key*, page 26
- *Defining general system settings*, page 26
- *Setting up notifications*, page 29
- *Configuring linking*, page 31
- *Configuring system modules*, page 32
- *Running the first-time policy wizard*, page 36
- *Reviewing and deploying changes*, page 22

To get Websense Data Security up and running, follow these basic steps:

1. Enter your Websense Data Security subscription key.
2. Define the general system settings, such as user directories and alerts.
3. Set up notifications.
4. Configure the system modules.
5. Run the first-time policy wizard.
6. Deploy your settings.

If you have Websense Web Security Gateway Anywhere, follow these steps:

1. Define the general system settings, such as user directories and alerts.
2. Configure linking with Websense Web Security.
3. Run the first-time policy wizard.
4. Deploy your settings.

Basic instructions are provided in this chapter. For more detailed instructions, follow the links under **Related topics**.

Entering your subscription key

Related topics:

- *Entering subscription settings*, page 225

Before beginning to work with the Websense Data Security you must enter your subscription key:

1. Log on to TRITON - Data Security. If you have never entered subscription information before, the subscription page appears automatically. If you need to navigate to the subscription page:
   a. Select **Settings** > **Configuration** > **System**.
   b. From the System pane, choose **Subscription**.
2. Select the product to which you subscribe:
   - Data Security Suite
   - Websense Web Security Gateway Anywhere
3. If you select Data Security Suite, browse to your subscription file, then click **Submit**. Your current subscription information is displayed, and the TRITON - Data Security application restarts.
4. If your license is about to expire, you'll see a notice in this screen, along with an Update button. Click the **Update** button to update your subscription. Once updated, you'll need to log off and then log on again to see accurate information on the subscription screen.

✓ **Note**

If you have Websense Web Security Gateway Anywhere, enter your subscription information in TRITON - Web Security or Content Gateway Manager. It is communicated to the Data Security Management Server automatically.

Defining general system settings

Related topics:

- *Configuring user directory server settings*, page 27
- *Setting up alerts*, page 28
- *Configuring System Settings*, page 209

On the **Settings** tab, there are settings to configure before you can get started. Namely, you need to:

- Configure user directory server settings. This lets you base your administrator logon authentication on user directory credentials, resolve user details during analysis, and enhance the details displayed with the incident.
- Set up alerts. This lets you configure the cases when administrators receive alerts from the system, such as when a subscription is about to expire or disk space is reaching its limit.

Configuring user directory server settings

Related topics:

- *Configuring user directory settings*, page 215

1. Select **Settings** > **Configuration** > **System**.
2. Click the **User Directories** option in the System pane.
3. Click **New** in the toolbar.
4. In the Add User Directory Server screen, complete the following fields:

Field	Description
Name	Enter a name for the user directory server.
Type	Select the type of directory from the pull-down menu: Active Directory, Domino, ADAM, or CSV file.
Follow referral	Select **Follow referral** if you want Websense Data Security to follow server referrals should they exist. Otherwise, select **Ignore referrals**. A server referral is when one server refers to another for programs or data.
Connection Settings	
IP address or host name	Enter the IP address or host name of the user directory server.
Port	Enter the port number of the user directory server.
User name	Enter a user name that has access to the directory server.
Password	Enter the password for this user name.
Use SSL Connection	Select this box if you want to connect to the directory server using Secure Sockets Layer (SSL) encryption.
Test Connection	Click this button to test your connection to the user-directory server.
Directory usage	

Field	Description
Import user records from this server	Select this option if you want to import user and group information from the specified directory server to your resource page. If you do not select this box, you cannot add these resources to your policies.
Get additional user attributes	Select this box if you want to retrieve additional user attributes from the directory server.
Attributes to retrieve	Enter the user attributes that you want TRITON - Data Security to collect for all users (comma separated).
Sample email address	Enter a valid email address with which you can perform a test.
Test Attributes	Click **Test Attributes** to retrieve user information on the email address you supplied. Click **View Results** to check the user information imported.
Use this server to authenticate logged-in administrator	Select this option if you want to authenticate administrators on this server when they log on to TRITON - Data Security.

5. Click **OK** to save your changes.

✓ **Note**

If you select CSV as the file type in the Add User Directory Server, you won't see the IP address, port, and SSL fields. You need to supply the full path for the CSV files, along with a user name and password. The Test Connection functionality is the same.

There are no Directory usage fields associated with CSV files.

Setting up alerts

Related topics:

- *Configuring alerts*, page 222
- *Setting up email properties*, page 223

1. Select **Settings** > **Configuration** > **System**.
2. Select the **Alerts** option in the System pane.
3. On the **General** tab select the conditions on which you want to trigger alerts.

4. On the **Email Properties** tab, complete the fields as follows:

Field	Description
Sender name	When an alert is sent to administrators, from whom should it be coming?
Sender email address	Enter the email address of the person from whom the alert is coming.

5. To define or edit the **Outgoing mail server**, click Edit (the pencil icon). Complete the fields as follows:

Field	Description
IP address or host name	Enter the IP address or host name of the outgoing SMTP mail server to use for scheduled alert notifications.
Port	Enter the port number of the mail server to use.

6. Complete the remaining fields as follows:

Field	Description
Subject	Enter a subject for alerts. Click the right-arrow to select a variable to include in the subject, such as %Severity%.
Recipients	Click **Edit** to select the recipients to whom alerts should be sent.

7. Click **OK** to save your changes.

✓ **Note**

The same outgoing mail server is used for alerts, notifications, and scheduled tasks. The settings you use here apply to the other cases, and if you change the settings for one, it affects the others.

Setting up notifications

✓ **Note**

If you have Websense Web Security Gateway Anywhere, this step does not apply to you.

Notification are configured on the **Resources** page. Notifications are email messages that are sent when policy breaches are discovered.

Websense Data Security offers a built-in notification template, **Default notification**, that you can edit as required. This notification is used as a default by the built-in action plans: to ensure that a notification is sent when an action plan is triggered, either edit the Default notification or create a new notification and edit your action plan to use it. See *Notifications*, page 119 and *Action Plans*, page 112 for more details.

1. Select **Main** > **Policy Management** > **Resources**.
2. From the Remediation section, select the **Notifications** option.
3. Click **New** on the toolbar.
4. Enter a name and description for this notification template, such as “Breach notification”.
5. On the **General** tab, complete the fields as follows:

Field	Description
Sender name	Enter the name of the person from whom notifications should be sent. This is the name that will appear in the email **From** field.
Sender email address	Enter the email address of the person from whom notifications should be sent.

6. You already configured the outgoing mail server when setting up alerts. The same server is used for notifications and scheduled tasks. There is no need to change this here.
7. Complete the remaining fields as follows:

Field	Description
Subject	Type the subject of the notification. This appears in the email **Subject:** line. Click the right arrow to choose variables to include in the subject, such as “This is to notify you that your message was %Action Taken% because it breached corporate policy.”
Recipients	Define the recipient(s) for the notification. Click **Edit** to select to select users or groups from a user directory. Select **Additional email addresses** then click the right arrow to select a dynamic recipient that varies according to the incident. For example, you can choose to send the notification to the policy owners, administrators, source, or source’s manager. Select the variable that applies, such as %Policy Owners%.

8. On the **Notification Body** tab, select a notification type and display format from the drop-down lists.

Field	Description
Type	For fastest set up, select **Standard** and leave all the check boxes selected. See *Notifications*, page 119 if you want to customize notifications.
Display as	Select a display format from the drop-down list: HTML or plain text.

9. Click **OK** to save your changes.

Configuring linking

Related topics:

◆ *Linking data and Web security*, page 226

✓ **Note**

This step applies only to customers with Websense Web security solutions (Websense Web Filter, Web Security, Web Security Gateway, or Web Security Gateway Anywhere).

In order to include URL categories in policies or perform IP address to user name resolution for incidents, you must configure linking and enable the Websense Linking Service. You can configure this in the TRITON - Data Security or TRITON - Web Security user interface. If you have configured linking in the Websense Web Security product, you do not need to do it here as well.

To configure linking in TRITON - Data Security:

1. Select **Settings** > **Configuration** > **System**.
2. From the System pane, choose **Linking**.
3. Enter the IP address and port as follows:

Field	Description
IP address or host name	Enter the IP address or host name of the TRITON - Web Security machine (also known as the Web Security Manager machine).
Port	Enter the port number of the TRITON - Web Security machine.

4. Click **Link**. This creates a connection between TRITON - Data Security and TRITON - Web Security.

   When you click **Link**, TRITON - Data Security looks for the Websense Linking Service and enables it. It displays the IP address and port number for the Linking Service that it found in the Linking Service section of the screen.

   If it cannot find the Linking Service, this information is not displayed. Refer to *Linking Service information is not shown on the Linking page*, page 309 for troubleshooting tips.

5. Click **Test Connection** to test the linking connection. A confirmation message is returned.
6. Click **OK**.

For information on enabling the module tray buttons, importing URL categories, or editing or disabling Linking Service properties, see *Linking data and Web security*, page 226.

Configuring system modules

Related topics:

- *Managing System Modules*, page 243
- *Configuring the protector*, page 33

✓ **Note**

If you have Websense Web Security Gateway Anywhere, this step does not apply to you.

When you install Websense Data Security, the modules you install are automatically registered with the Data Security Management Server.

Select **Settings** > **Deployment** > **System Modules** to view a list of all the modules you installed.

The Data Security Management Server has the following modules by default:

- SMTP agent
- PreciseID fingerprint repository
- Endpoint server
- Crawler (fingerprinting and data discovery agent)
- Forensics repository
- Policy engine

The protector appliance has the following modules:

- ICAP agent
- Policy engine
- PreciseID fingerprint repository

It is also a module itself.

If added any other modules to your system—such as supplemental Data Security servers, agents, crawlers, or the Websense Content Gateway—these components appear in the tree view as well.

To get Websense Data Security up and running, all you have to do is configure the protector. You need only configure the other modules for non-default behavior. In some cases, the protector is not even required—as in some endpoint deployments and in Websense Web Security Gateway Anywhere deployments.

> ✓ **Note**
> See the *Websense Data Security Deployment Guide* for instructions on installing Websense Data Security modules.

Configuring the protector

> ✓ **Note**
> Refer to *Configuring modules*, page 246 for information on the default settings of system modules.

1. Select **Settings** > **Deployment** > **System Modules**.
2. If it is not already, expand the tree in the content pane.
3. Click the protector module in the tree and provide the information in all the tabs offered:
   - *General tab*, page 33
   - *Networking tab*, page 34
   - *Local Networks tab*, page 35
   - *Services*, page 35

General tab

Field	Description
Name	The name you gave the protector when you added it. Edit as desired.
Description	The description you gave the protector when you added it. Edit as desired.

Field	Description
Enabled	Select **Enabled** to activate this protector in your system. Though you have added the protector, it is not used until you select **Enabled**.
Host name	Read-only field of current host name.
IP address	Read-only field of current IP address.
Managed by	Enter the name of the Data Security Management Server that should manage this protector.

Networking tab

Field	Description
Default gateway	Enter the name of your default network gateway. This is the gateway that your computer uses when it needs to route data to a network that is not directly accessible (for example, it's in a different VLAN).
Interface	Select the type of network interface being used for this protector.
DNS servers	Enter the IP address of your network Domain Name System (DNS) server, then click **Add**. If you have more than one DNS server, add them all.
DNS suffixes	Enter the DNS suffix used by your organization, then click **Add**. If you have more than one DNS suffix, add them all.
Connection mode	Select a connection mode from the drop-down list to indicate how you have deployed this protector. Was it deployed in inline (bridge) or SPAN/mirror port mode?

Field	Description
Network interfaces	There are 4 types of network interfaces: Management, Bridge, Monitoring, and Network. Click an interface to view or change details about it. A dialog appears. Depending on the interface, you might be asked to enter the following: ◆ **Interface name** - The name of the network interface. ◆ **Status** - Set the status of the interface to Up or Down. ◆ **Mode** - Select Network or Monitoring ◆ **Interface IP address** - Enter the interface's IP address. ◆ **Subnet mask** - Enter a subnet mask for the interface. ◆ **Link speed** - Set the Link Speed to either: 10Mb/s, 100 Mb/s, 1000Mb/s, Automatic. ◆ **Duplex mode** - Set Duplex Mode to either Half, Full or Automatic. ◆ **Bridge name** - The name of the network interface. ◆ **Enable bypass mode** - Select this option to activate bridge failover. ◆ **Force bypass** - Select this option to force bridge into bypass mode.
Enable VLAN support	Select this check box if you want to enable Virtual LAN support on this network.

Local Networks tab

Field	Description
Include all networks	Select this radio button to cover all local networks with the protector. Note that when you select this option, the protector accepts all traffic it sees for processing, regardless of the Direction setting on the Services tab.
Include specific networks	Select this radio button to specify which local networks to cover, then specify the following: ◆ **Network address** - Specify the network IP address to include. ◆ **Subnet mask** - Specify the network subnet mask to include. Click **Add**.

Services

Select the services you want the protector to monitor or add a new service. The **Services** tab indicates whether incoming, outgoing, or internal data is to be monitored (unless you selected **Include all networks** above, in which case all traffic is monitored regardless). In most cases, the default settings are sufficient to get you started.

To change the default settings, click a service name or highlight a name and click **Edit**. Refer to *Configuring the protector*, page 255 for information on configuring protector services.

Running the first-time policy wizard

Once you have installed Websense Data Security software and defined an administrator, the next step is to create a policy.

Websense Data Security comes with a rich set of predefined policies that cover the data requirements for a variety of regulatory agencies (such as GLBA, HIPPA, and Sarbanes-Oxley) all over the globe. For each policy, there is a template that was composed in accordance to specific regulations or acts. The template is an XML document that defines policy content.

Websense Data Security provides a policy wizard that allows you to select predefined policies to monitor and control the communication of customer data and company confidential information according to specific laws and regulations.

To create your first policy:

1. Select **Main** > **Policy Management** > **Data Usage Policies**.

   or

   Main > **Policy Management** > **Data Discovery Policies**.

   Choose the first option to create a policy that protects data in your network or endpoint systems.

   Choose the second option to create a policy that will discover the location of sensitive data in your enterprise.
2. Read the **Welcome** screen and click **Next** when you're ready to proceed.
3. In the **Regions** screen, indicate the region or regions for which you will be creating policies. This helps the policy wizard focus on policies generally relevant to your geographical location. Expand the tree by clicking the plus signs. Click **Next** when you're done.
4. In the **Industries** screen, select the industry or industries relevant to the policies you will create. This helps the policy wizard focus on policies generally relevant to your industry.

   If the policies are to be run at a public company, select the **Public Company** check box to ensure all policies relevant to public companies are available.
5. Click **Next**. The **Policies Templates** screen appears showing policies that may be relevant for your organization. Highlight a policy to read details about it. You can view all relevant policies or only those that are commonly used. (For more information about these regulatory compliance policies, refer to *Predefined Policies*, page 317.)
6. Select the policies you want to apply in your organization by checking the box next to their policy names. When you are satisfied with the policies you have selected, click **Next**.

7. The **Finish** screen appears, summarizing your selections. Click **Finish**. The Websense Data Security policy database is updated and a confirmation message appears.

Many times, these predefined regulatory policies are all our customers need to deploy. However, once you are accustomed to monitoring incidents from these mission-critical policies, you may choose to create custom policies to safeguard other types of data as well—for example, proprietary data on file servers and SharePoint.

You create custom policies using wizards as well. Refer to Chapter 4 for information on creating policies for your network and endpoint machines. Refer to Chapter 5 for instructions on creating data discovery policies.

✓ **Note**

The Regions and Industries settings you configured in this section are applied to data discovery policies as well as data usage. You do not need to select them again. If you want to change them in the future, go to the policies view, click **Policy Templates** then click **Filter**.

⚠ **Warning**

If you customize one of Websense's built-in policies and save it under a new name, you are responsible for keeping that policy up to date.

Deploying your settings

To deploy all the settings and policies you configured in this chapter, click **Deploy** in the TRITON - Web Security toolbar.

Part II

Securing Your Company's Data

4 Creating Custom Policies

Related topics:

- *What's in a policy?*, page 41
- *Viewing policies*, page 43
- *Creating a custom policy*, page 49

Once you've had an opportunity to run your regulatory policies for a while and monitor the results, you might want to create custom policies.

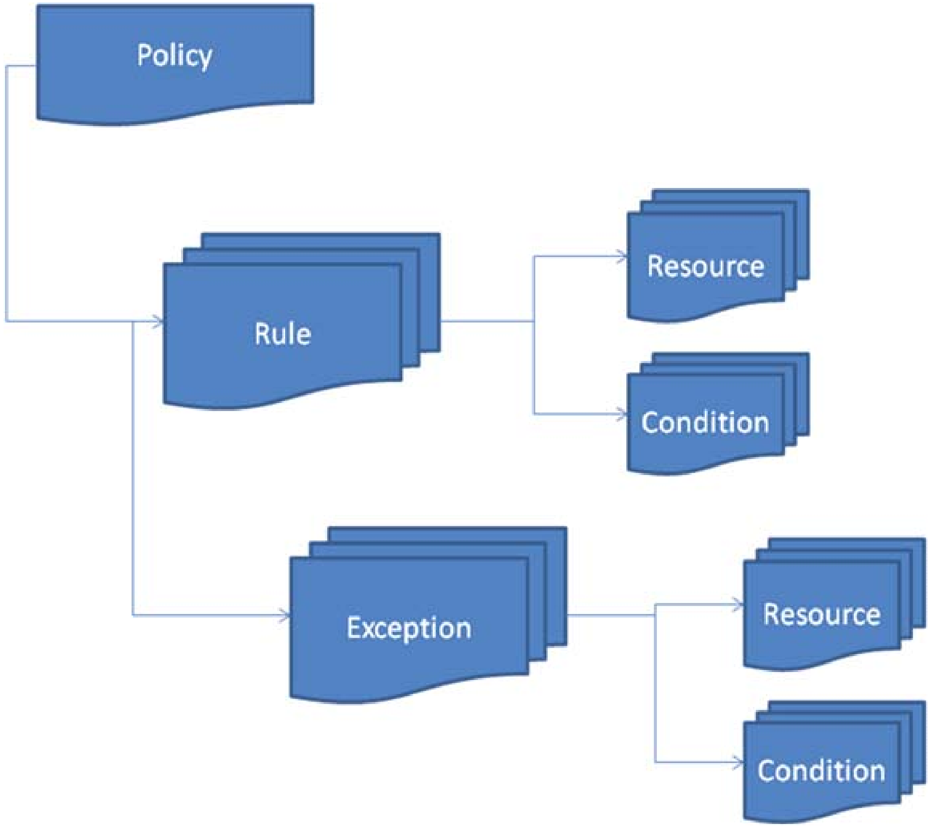
Although much of this process is performed through wizards, it's important that you understand some key concepts before you get started.

What's in a policy?

Related topics:

- *Managing rules*, page 62
- *Adding exceptions*, page 62
- *Classifying Content*, page 69
- *Defining Resources*, page 101

In Websense Data Security, policies contain rules, exceptions, conditions (defined by content classifiers), and resources. This is true of predefined and custom policies.



Element	Description
Rules	Provide the logic for the policy. They are the conditions that govern the behavior of the policy. When should something be blocked? When should managers be notified?
Exceptions	Define the conditions that should be exempt from the rules. An exception is part of a rule and checked only when its rule is triggered.
Content classifiers	Describe the data to be governed. You can classify data by file properties, key phrases, dictionaries, natural language processing (NLP), a database record fingerprint, a directory fingerprint, and/or a file fingerprint.
Resources	Describe the source and destination of the data you want to protect, the endpoint device or application that may be in use, and the remediation or action to take when a violation is discovered (such as *block* or *notify*).

These components are the building blocks of a policy. When you create a policy from a regulatory template, it contains rules, exceptions, classifiers, sources, destinations, and actions already. When you create a policy from scratch, wizards prompt you for such information.

Data discovery policies also contain data discovery tasks. These describe where to perform the discovery. On networks, this may include a file system, SharePoint directory, database, or Exchange server. If you're performing endpoint discovery, it includes the exact computers to scan.

Viewing policies

Related topics:

- *Tree icons*, page 44
- *Policy levels*, page 46

Select **Policy Management > Data Usage Policies** or **Data Discovery Policies** from the **Main** tab to view a list of policies that have been defined for your organization.

If you have not yet run the first-time policy wizard, it appears. (See *Running the first-time policy wizard*, page 36 for more information.)

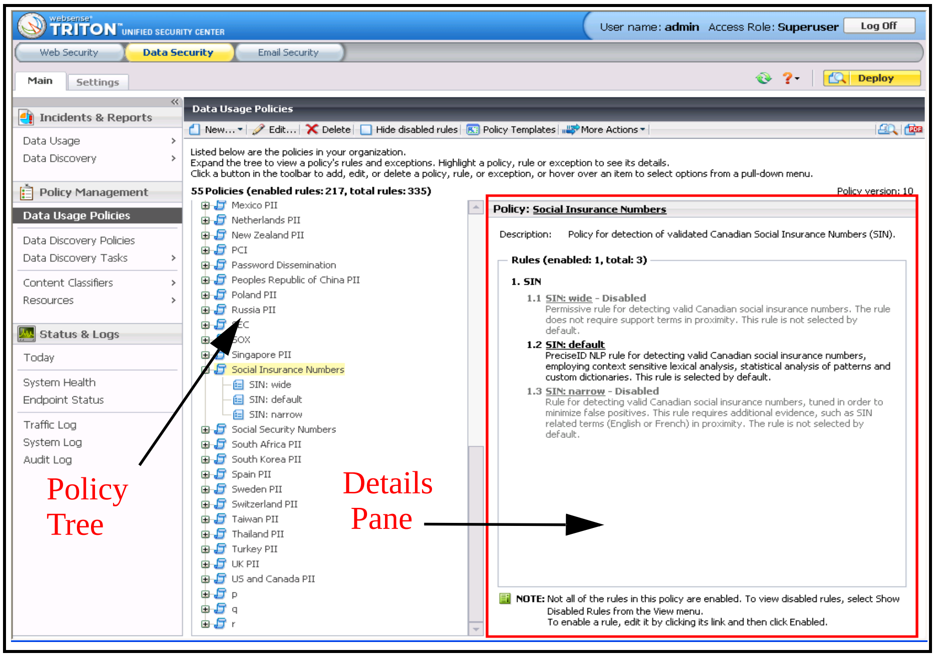
Policies appear in a tree-view structure in alphabetical order under their assigned level, if any. You can add policies any time. Each policy consists of a set of rules and a possible set of exceptions.

The branches in the tree can be expanded to display the items relevant to that component. Under levels, there are policies. Under policies, there are rules. And under rules, there are exceptions. To expand a branch, click the plus sign (+) next to the desired component. To collapse a branch, click the minus sign (-) next to the desired component.

Select a policy, rule, or exception to view descriptive information about it in the **Details** pane. A policy description and a description of the rules that the policy contains display. Scroll down to view all the information that is available. Click **Advanced** to see what the sources and destinations are.

When you select a rule, the right pane displays a description, the condition, and exceptions.

And when you select an exception, it displays a description, the condition, and the action.



Listed below are the policies in your organization.
Expand the tree to view a policy's rules and exceptions. Highlight a policy, rule or exception to see its details.
Click a button in the toolbar to add, edit, or delete a policy, rule, or exception, or hover over an item to select options from a pull-down menu.

55 Policies (enabled rules: 217, total rules: 335)

Policy: Social Insurance Numbers

Description: Policy for detection of validated Canadian Social Insurance Numbers (SIN).

Rules (enabled: 1, total: 3)

1. SIN

1.1 SIN: wide - Disabled
Permissive rule for detecting valid Canadian social insurance numbers. The rule does not require support terms in proximity. This rule is not selected by default.

1.2 SIN: default
PreciseID NLP rule for detecting valid Canadian social insurance numbers, employing context sensitive lexical analysis, statistical analysis of patterns and custom dictionaries. This rule is selected by default.

1.3 SIN: narrow - Disabled
Rule for detecting valid Canadian social insurance numbers, tuned in order to minimize false positives. This rule requires additional evidence, such as SIN related terms (English or French) in proximity. The rule is not selected by default.

NOTE: Not all of the rules in this policy are enabled. To view disabled rules, select Show Disabled Rules from the View menu.
To enable a rule, edit it by clicking its link and then click Enabled.

Tree icons

The following icons are used to represent policy data in the tree structure:

Icon	Description
	Level (See *Policy levels*.)
	Policy
	Rules
	Exception

The policy toolbar

The policy toolbar provides many functions. You can access these same functions by hovering over a policy, rule, or exception, then selecting an option from a pull-down menu. For example, click a policy and you can edit or delete it by selecting **Edit** or

Delete from the pull-down menu. click a rule, and you can add a new exception by selecting **New** > **Exception**.

Button	Description
New… ▾	Create a new policy, rule, or exception.
Edit…	Edit the selected policy, rule, or exception.
✗ Delete	Delete the selected policy, rule, or exception. The administrators that were directly assigned to this policy see it in their policy list as deleted. They continue to see old incidents that relate to this policy, however. If you do not want to see incidents for a deleted policy, uncheck the policy in your Incident report list.
☑ Show disabled rules	Show or hide disabled rules in the policy tree.
Policy Templates	Lists the predefined policy templates that have been applied to your organization. You can change the filter to redefine regions or industries, and you can choose new regulatory policies. You can also install updates to your predefined policies, rules, and classifiers.
More Actions ▾	• **Batch Operations** - lets you update or delete multiple items at once. For example, select **Update All Rules of Current Policy** to go to a Update Rules pane where you can change the fields for all the rules of a selected policy at once, or for selected rules. This overrides the settings in the policy and reduces time and effort involved. Select **Update All Exceptions of Current Rule** to change specific exceptions or all exceptions in a selected rule. Select **Update Rules** to make changes to selected rules or all rules across all policies, and select **Update Exceptions** to change selected exceptions or all exceptions across all rules. Select **Delete Policies** to delete a batch of policies at once: a screen appears so you can choose which policies to delete. • **Rearrange Exceptions** - lets you set the order of exceptions under the selected rule. • **Manage Policy Levels** - lets you manage policy levels.
	Displays a formatted Print Preview of all levels, policies, rules, and exceptions.
	Exports policy data to a PDF file. You can export the current policy, all policies from this level, or all policies. Policies, rules, and exceptions are exported.

The information icon ⓘ , when present, lets you see additional details about a field.

Note
Not all rules are configurable. You cannot edit rules that were predefined in the regulatory templates that Websense provides.

Policy levels

Related topics:

- *Adding a new policy level*, page 46
- *Deleting a policy level*, page 47
- *Rearranging policy levels*, page 47
- *Rearranging exceptions*, page 63

When you create policies, you can assign them a level that indicates execution priority order. The tree structure demonstrates the hierarchy that has been assigned. You can have as many levels as you wish. When you create a policy level, you assign it a name and an execution order.

For example, you may create 3 levels called High, Medium, and Low, where high-level policies are executed first, medium-level policies second, and low-level policies last. If there is a match when data is scanned according to the high-level policies, no scanning is performed on other levels. (Policies on the high level are still checked.) If there is no match, data is scanned according to medium-level policies, and so on.

At first when you install Websense Data Security, you have just one priority level. All the policies are implemented and the action is taken accordingly.

Adding a new policy level

1. Select **More Actions > Manage Policy Levels** from the policy window. The Manage Policy Levels dialog appears.
2. Click **New** from the menu bar to add a new policy level.
3. Enter a level name and description into the Add/Edit Level dialog. You can name the levels anything you want. For example, the military might define top secret, confidential, secret levels. If an incident matches a policy on the top-secret level, Websense Data Security quits searching for matches on confidential policies.
4. Click **Select from list** on the lower-right corner of the dialog to select policies to add to this level.
5. Select the policy name(s) of interest in the left pane and click **Add>>** to move it into the right pane.
6. Click **OK** to confirm the action.

Deleting a policy level

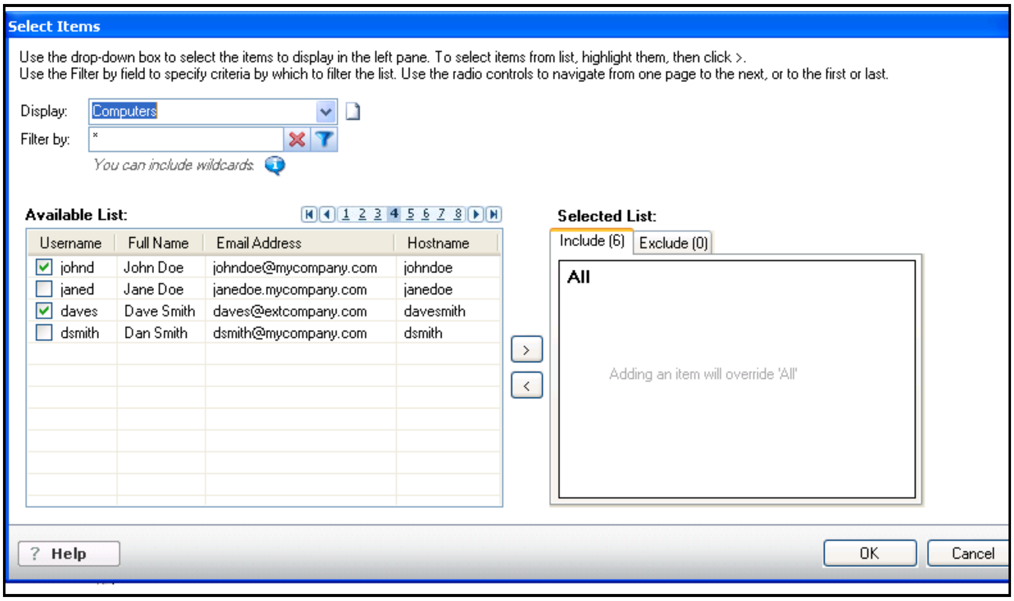
1. Select **More Actions** > **Manage Policy Levels** from the policy window. The Manage Policy Levels dialog appears.
2. Select the level of interest by checking the box next to it.
3. Click **Delete** from the menu bar.
4. Click **OK** to confirm the action.

Rearranging policy levels

1. Select **More Actions** > **Manage Policy Levels** from the policy window. The Manage Policy Levels dialog appears.
2. Highlight the level of interest.
3. Click **Rearrange Levels** from the menu bar.
4. Use the up and down arrows to change the order of the levels you created.
5. Click **OK** to confirm the action.

Selecting items to include or exclude in a policy

In TRITON - Data Security, whenever you need to select items to include in a policy, such as sources, destinations, channels, actions, or any other items, a selector tool appears. For most operations—selecting application names, content classifier names, or files, for example—the selector looks like this:



Select Items

Use the drop-down box to select the items to display in the left pane. To select items from list, highlight them, then click >.
Use the Filter by field to specify criteria by which to filter the list. Use the radio controls to navigate from one page to the next, or to the first or last.

Display: Computers

Filter by: *

You can include wildcards

Available List:

	Username	Full Name	Email Address	Hostname
☑	johnd	John Doe	johndoe@mycompany.com	johndoe
□	janed	Jane Doe	janedoe.mycompany.com	janedoe
☑	daves	Dave Smith	daves@extcompany.com	davesmith
□	dsmith	Dan Smith	dsmith@mycompany.com	dsmith

Selected List:

Include (6) Exclude (0)

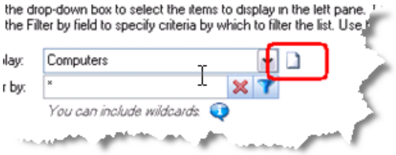
All

Adding an item will override 'All'

The selector is used to select which entities you want to include in the rule and which you want to exclude. Say you want users in the group Finance to be able to move, copy, and print corporate financial data in the /finance directory. You would select the group Finance with the Sources selector and you would select the directory /finance with the Destinations selector. Perhaps there is one exception—you do not want Finance user bsmith to have these privileges. On the Sources selector, you would add this user to the exclusions list.

You may have one or more exclusions to a rule. For example, perhaps Finance users should be able to copy data from all finance directories except /finance/executives (you would add these directories from the exclusions list on the Destinations selector), and you want to block bsmith from copying data.

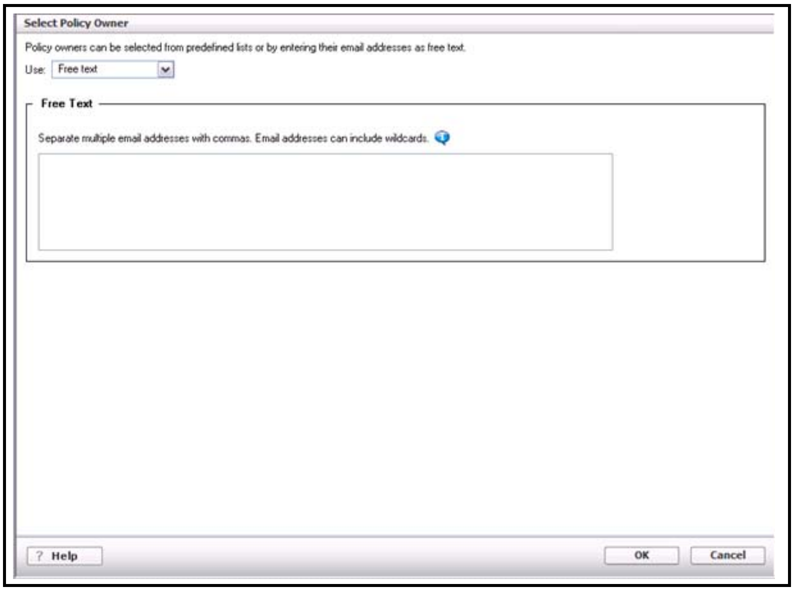
To use the selector, complete the fields as follows:

Field	Description
Display	Select the entity—such as computers or networks if you are selecting a source—to display in the **Available List** box at the bottom of the page. If you do not see what you want to display, in some cases you can create a new resource by clicking the paper icon.  the drop-down box to select the items to display in the left pane. the Filter by field to specify criteria by which to filter the list. Use lay: Computers r by: * You can include wildcards See *Defining Resources*, page 101 for instructions.
Filter by	Typically too many entries are available to display on one page. Use the **Filter by** field to specify criteria by which to filter the list, such as “*jones*”. You can use wildcards in your filter string if desired. “?” represents any single character, as in the example “file_?.txt”. “*” represents zero or more of any character, such as “*.txt”. Click the **Apply filter** button to apply the filter or the **Clear** button to clear it.
Available List	Lists the items that are available for selection in the current display category. Use the page forward/backward controls to navigate from one page to the next, or to the first or last page. In some cases, a folder icon or up arrow appears. Click the icon to display the directory one level up in the directory tree. You can also click the breadcrumbs above the list to navigate to another level.
Selected List	Use the right and left arrows to move items into and out of the selected list. If you want to include a computer named Bob_Computer, highlight it on the left, make sure the **Include** tab is active, and click >. If you want to exclude Bob_Computer, make sure the **Exclude** tab is active when you click >. **Tip:** you can move a group of users, computers, networks, etc. into the **Include** box, then remove one user, computer, or network by highlighting it on the right and clicking **Remove**.

When you are selecting sources or destinations, however, you can select items from predefined lists or enter free text to identify the items to include in the policy.

On the sources and destinations selector:

1. From the pull-down list, select **Predefined lists** if you want to select from lists or select **Free text** to type the name of an item to include.
2. If you choose **Predefined lists**, complete the fields in the table above. If you choose **Free text**, a box appears:



Select Policy Owner

Policy owners can be selected from predefined lists or by entering their email addresses as free text.

Use: Free text

Free Text

Separate multiple email addresses with commas. Email addresses can include wildcards.

In the space provided, type the entity you want to include. For example, if you are selecting a source, type the desired owner's email address. If you're selecting a computer, type the computer name or IP address. You can enter multiple items. If you do, separate them with commas. For example:

```
ssmith@example.com, mjones@example.com
```

Wildcards are allowed.

3. Click **OK**.

Creating a custom policy

Related topics:

- *Using express mode*, page 51
- *Using advanced mode*, page 53
- *Managing rules*, page 62
- *Adding exceptions*, page 62
- *Defining Resources*, page 101
- *Running the first-time policy wizard*, page 36

After you create a regulatory policy using the first-time policy wizard, you may want to create custom policies as well.

To create a custom policy, do the following:

1. From the **Main** tab, select **Policy Management > Data Usage Policies** if you want to create a policy to govern data in motion across your network or on endpoint machines.

   or **Policy Management > Data Discovery Policies** if you want to create a policy responsible for discovering the location of sensitive data in your network.
2. In the toolbar, click **New > Policy**.
3. Complete the fields as follows:

Field	Description
Policy name	Enter a name for this policy, up to 256 characters.
Enabled	Select this check box to enable the policy in your organization. Deselect it if you plan to enable it later. Policies can be deployed in an enabled or disabled state. Only enabled policies are applied across your organization.
Description	Optionally, provide a description of this policy, up to 4000 characters.
Policy owners	By default, no policy owners are included in the policy. To define a policy owner(s), click **Edit**. In the resulting box, select the people who should receive notification in the event of a policy breach. Click the right-arrow to move them into the Selected List. These are known as *policy owners*. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool.

4. Click **OK**. The Create a Rule dialog box appears, because all policies must contain at least one rule.
5. Indicate whether you want to use express or advanced mode to create the rule. Express mode handles most of your needs.

Field	Description
Express mode	Select this mode if you want to accept the default rule properties for your data. See *Using express mode*.
Advanced mode	Select this if you want to specify rule properties using a wizard. See *Using advanced mode*.
I don’t want to create a rule now	Select this if you want to create a rule later. you can add one any time by highlighting a policy and clicking New Rule.

Using express mode

In express mode, you identify your data using content classifiers and let Websense Data Security create the rule for you.

You can create a new content classifier or choose an existing one.

1. Under **Create a Rule in Express Mode**, select one of the following radio buttons:

Field	Description
Help me create a new content classifier	Select this button if you have unique data and know how to define it.
Let me select from existing content classifiers	Select this button to choose from dozens of common, predefined classifiers, such as: ◆ PreciseID patterns > Credit Card Numbers (AmEx) ◆ PreciseID patterns > SSN with delimiters (See Appendix B: *Predefined Classifiers*, page 341 for a description of each predefined classifier.)

2. Select a classifier type for this rule.

   If you selected **Help me create a new content classifier**, your options are:

Type	Description
PreciseID Patterns	Lets you classify data by regular expression patterns. Used to identify alphanumeric strings of a certain format, such as 123-45-6789.
Key Phrases	Lets you classify data by the presence of a keyword or phrase, such as “confidential.”
Dictionaries	Lets you classify data using terms that belong to a certain knowledge domain, such as medical or financial terms.
File Properties - by type	Lets you classify data by file type. File type identifies files by metadata.
File Properties - by name	Lets you classify data by file name. File name identifies files by their extension or file name.
File Properties - by size	Lets you classify data by file size.

If you selected **Let me select from existing content classifiers**, you have additional options:

Type	Description
PreciseID Natural Language Processing (NLP)	Lets you classify data by context. Used for numeric data such as credit card numbers or scientific data such as software design documents and source code.
PreciseID fingerprinting - files and directories	Lets you fingerprint files or directories, including SharePoint directories.
PreciseID fingerprinting - database records	Lets you fingerprint database records.

✓ **Note**

If you want to create a new fingerprinting classifier, see *PreciseID Fingerprinting - files & directories*, page 84 or *PreciseID Fingerprinting - database records*, page 89.)

3. Click **OK**.
4. If you chose **Help me create a new classifier**, an **Add Classifier** box appears. Click a link below for instructions on completing the fields for the type of classifier you chose:
   - *PreciseID Patterns*
   - *Key Phrases*
   - *Dictionaries*
   - *Adding a file-type classifier*
   - *Adding a file-name classifier*
   - *Adding a file-size classifier*

   If you chose **Let me select from existing classifiers**, a **Select Classifier** box appears. Select the predefined content classifier to add to this rule.
5. Click **OK**, and a rule is created for the classifier you defined. It is automatically added to your new policy. A confirmation message appears.

Using advanced mode

Related topics:

- *Rule Wizard - General*, page 53
- *Rule Wizard - Condition*, page 54
- *Rule Wizard - Severity & Action*, page 57
- *Rule Wizard - Source*, page 58
- *Rule Wizard - Destination*, page 59
- *Rule Wizard - Finish*, page 61

Advanced mode gives you more control over the properties of the rule you're creating. It lets you define the condition, severity, action plan, source, and destination for the rule. There are 6 pages in the advanced mode wizard:

- *General*
- *Condition*
- *Severity & Action*
- *Source*
- *Destination*
- *Finish*

Complete the information on each page and click **Next** to proceed through the wizard.

Websense recommends that you initially set your policy to apply to all sources and destinations of data with a permissive action. Later, you can permit or block certain sources and destinations and apply more restrictive actions. If you intend to customize these resources in your policy, you must configure them first under **Policy Management** > **Resources**.

Rule Wizard - General

Related topics:

- *Rule Wizard - Condition*, page 54

Field	Description
Policy name	The name for this policy.
Rule name	Enter a name for this rule.

Field	Description
Enabled	Select this box to enable the rule for this policy. If this box is unselected, the rule is present, but disabled.
Description	Enter a description for this rule.

Rule Wizard - Condition

Related topics:

- *Classifying Content*, page 69
- *Rule Wizard - Severity & Action*, page 57

The **Condition** tab defines the logic of the rule.You can select one or more content classifier conditions, and you can generate logic between the conditions using and, or, not, and parentheses. This logic should be based on your business rules. (See the example below the table.)

Field	Description
This rule monitors	• **All activities** - Select this option to trigger the rule on any content without analysis. For example, you may want to specify that any content that your CEO sends is allowed. • **Specific data** - Select this option to monitor specific data, then define the specific classifier(s) to use.

Field	Description
Add	Initially, you may have no conditions defined. To add one, click **Add**, then select the type of condition to add: - **PreciseID Pattern** - Lets you classify data by regular expression patterns. - **Key Phrase** - Lets you classify data by the presence of a keyword or phrase, such as “confidential.” - **Dictionary** - Lets you classify data using terms in industry dictionaries, such as medical or legal terms. - **File Properties** - Lets you classify data by file types, file name extensions, or file size. - **PreciseID Natural Language Processing** - Lets you classify data using natural language processing scripts provided by Websense. - **PreciseID Fingerprinting - Files & Directories** - Lets you fingerprint files or directories, including SharePoint directories. - **PreciseID Fingerprinting - Database Records** - Lets you fingerprint database records. To delete a condition from the rule, select a condition and click **Remove.** To edit a condition’s threshold, that is, the number of matches that trigger an incident, click a hyperlink in the Threshold column. **Note:** You cannot edit a predefined content classifier.
Condition Relations	If you have more than one condition defined, select a condition relation: **And**, **Or**, or **Customized**. The condition relation determines how the conditions are related. - **And** - All of the selected conditions must be met to trigger the rule. - **Or** - One of the selected conditions must be met to trigger the rule. - **Customized** - Lets you define under what condition you want the rule triggered. If you choose **Customized**, do the following: 1. Click a condition name to add it to the formula box. 2. Click the **And**, **Or**, or **Not** button to define a condition. 3. Click another condition name. 4. Continue until you are done defining the condition. You can add parentheses, as in any mathematical operation. For example: `(1 AND 2) OR (3 AND 4) OR 5` The numbers relate to the condition number you have defined. 1 is the first condition; 2 is the second, and so on. Click the information icon on the right of the box to view a precise description of the condition you have defined.

Example

You are a bank and via a file fingerprinting classifier, you identify a blank application form. In your policy, you create a rule saying if this classifier is matched, permit it to be sent from all sources to all destination channels. The form is marketing. You want people to fill it out to apply for loans.

In the same policy, you create another rule: when the form contains a social security number and the word “income”, it is a loan application and should be permitted to go to one destination: the loan department. It should be blocked from all other destinations. The condition logic would state: when the fingerprinting classifier is matched AND a social security number PreciseID pattern is matched AND the keyword classifier “income” is matched, it is a standard loan application—`(1 AND 2 AND 3)`.

You can add a third rule to the policy: when content contains that same data plus the keywords “residential” or “deed” it is a mortgage application—`1 AND 2 AND 3 AND (4 OR 5)`. Permit it to be distributed to the mortgage department and title insurance partners.

Your conditions should be based on your business rules.

Rule Wizard - Severity & Action

Related topics:

- *Rule Wizard - Source*, page 58
- *Action Plans*, page 112

Field	Description
When the condition is matched, severity is:	Specify the severity of incidents that breach this rule: - **Low** - Incidents that match this rule are of low importance. The policy breach is minor. - **Medium** - Incidents that match this rule are of medium importance. The policy breach is moderate. - **High** - Incidents that match this rule are very important and warrant immediate attention. The policy breach is severe.
and the action plan is	Select an action plan for your policy. Action plans are customizable. By default, they include: - **Block all** - Select this option if you want this policy to use the strict actions defined under **Main > Policy Management > Resources > Action Plans**. - **Audit & notify manager** - Select this option (the default) if you want this policy to use the moderate actions defined. These are a compromise between strict and permissive actions. - **Audit only** - Select this option if you want this policy to use permissive actions. Click the pencil icon edit the action plan. You can change the action for each channel if desired. Editing an action plan changes it for all the rules that use it. Click the paper icon to create a new action plan. See *Action Plans*, page 112, for details.

Field	Description
Advanced	This option does not apply the Web Security Gateway Anywhere customers. Click **Advanced** to define severity at a more granular level. For example, when there are more than 10 matches, change severity to medium and action plan to audit & notify. When there are more than 20 matches, change severity to high and action plan to block. Select a check box and define the parameters as needed.
Define Matches	This option does not apply the Web Security Gateway Anywhere customers. Select how matches should be calculated: ◆ **Greatest number of** matched conditions. Select this option if you want the number of matches for each condition to be compared, and only the greatest number reported. For example, if there are 5 matches for the condition, ConfidentialPattern, 3 for SSN_Pattern, and 10 for MyKeyPhrases, the number of matches would be defined as 10. ◆ **Sum of all** matched conditions. Select this option if you want the number of matches for each condition to be added together and the total to be reported. Given the same example as above, the number of matches would be defined as 18.

Tip

Start with an action plan of audit. Once your policies are tuned, you can send notifications or block actions as needed.

Rule Wizard - Source

Related topics:

- *Rule Wizard - Destination*, page 59
- *Sources and destinations*, page 103

This page applies to data usage policies only. If you are creating a data discovery policy, this page does not appear.

Field	Description
Edit	By default, all sources of data are applied to this rule. Sources include computers, devices, domains, networks, etc. To select a source or sources, click **Edit**. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool.
Endpoints	◆ **Machine type** - Select the type of endpoint machines to analyze: all machines, all machines except laptops, or only laptops. ◆ **Network location** - Select the network location of the endpoint machines to analyze: machines anywhere, those connected to the corporate network, or those not connected to the corporate network. Use this field to define the behavior of endpoints when they are on and off network.

Rule Wizard - Destination

Related topics:

- *Rule Wizard - Finish*, page 61
- *What can I protect?*, page 2

This page applies to data usage policies only. If you are creating a data discovery policy, this page does not appear.

The Destination page varies depending on your subscription. You may see:

- *Standard options*
- *Web Security Gateway Anywhere mode*

Standard options

Field	Description
Email	Select the **Email** check box if you want to protect email channels. By default, email is analyzed on all destinations. Click **Edit** to select the destinations this policy should analyze. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool.
Web	Select this check box if you want to prevent or monitor users from posting sensitive data to Web channels. These include: ◆ **HTTP/HTTPS** - Web sites, blogs, and forums via HTTP and secure HTTP. ◆ **Endpoint HTTP/HTTPS** - Web sites, blogs, and forums accessed by endpoint machines over HTTP and HTTPS ◆ **FTP** - file transfer protocol (FTP) sites ◆ **Chat** - instant messenger applications ◆ **Plain text** - unformatted textual content By default, all Web destinations are analyzed. Click **Edit** to select the destinations to analyze. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool. Click **Advanced** to select or deselect individual Web channels.
Printing	Select this check box if you want to analyze files that are sent to printers, then select whether you want to monitor network printers or endpoint printers. (To monitor network printers, you must have a printer agent installed. To monitor endpoint printers, you must have the endpoint agent.) To select the printers to analyze click **Edit**. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool.
Endpoint Application	Select this check box if you want to analyze content that is being cut, copied, pasted, or otherwise handled by users on endpoint applications. To select the application groups to analyze, click **Edit**. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool. Not all operations (cut, copy, paste, etc.) relate to all applications. The operations that are monitored are specified for each group. Note that if you choose **All activities** on the rule's condition page and choose an online application here, you are requesting to monitor all content that is downloaded to endpoints. The same is true if you specify the Download operation in the online application group, then select this group. To prevent the system from analyzing content that is cached on the endpoint, the following occurs: ◆ When files are saved to the browser's cache folders, the crawler analyzes only .csv, .xls/xlsx, .pdf, .txt, .mht, and .doc/.docx files. ◆ When files are saved to any other local folder, it analyzes all file types.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Endpoint Removable Media</td><td>Select this check box if you want to analyze endpoint removable media, such as thumb drives, external hard drives, and other USB devices. By default, all removable media is included. To select the media to analyze, click <b>Edit</b>.
See <i>Selecting items to include or exclude in a policy</i>, page 47 for instructions on using the selector tool.</td></tr>
<tr><td>Endpoint LAN</td><td>Users commonly take their laptops home and then copy data through a LAN connection to a network drive/share on another computer.
Select this check box if you want to analyze endpoint file copy over LANs.
By default, outgoing traffic for all networks is covered—that is, traffic going from the endpoint to all LANs. To select a network to analyze, click <b>Edit</b>. See <i>Selecting items to include or exclude in a policy</i>, page 47 for instructions on using the selector tool.
With Websense Data Security:
◆ You can specify a list of IPs, host names, or IP networks of computers that are allowed as a destination for LAN copy.
Note that users may connect to the destination computer using any of these options, and Data Security does not resolve them. For this reason, if you want to block or allow access to a computer, you must specify it FQDN, host name, mapped drive, and any other address the user might use. Alternatively, always block or allow access using host name and inform your users to use host name.
◆ You can intercept data from an endpoint client.
Note that Endpoint LAN control is applicable to Windows File Sharing only.</td></tr>
</table>

Web Security Gateway Anywhere mode

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Edit</td><td>By default, Web channels are analyzed on all destinations. For Web Security Gateway Anywhere, this includes:
◆ <b>FTP</b> - file transfer protocol (FTP) or FTP-over-HTTP
◆ <b>Web</b> - Web sites, blogs, and forums via HTTP and HTTPS
Click <b>Edit</b> to select the destinations to analyze. See <i>Selecting items to include or exclude in a policy</i>, page 47 for instructions on using the selector tool.</td></tr>
</table>

Rule Wizard - Finish

Click **Next** to display a summary of the rule you just created. You can go back to make changes or click **Finish** to accept them.

If you select **Finish**, the new rule is added to the policy you selected.

Managing rules

Related topics:

- *Using express mode*, page 51
- *Using advanced mode*, page 53
- *Creating a rule from a content classifier*, page 99
- *Adding a new exception*, page 63

Rules define the logic of the policy. You can add them to, edit them, or delete them from a policy at any time. You can also enable or disable them.

After you create a policy using the express or advanced mode, you are prompted to create a rule automatically. You do so by creating a content classifier and Data Security creates a rule from that. (See *Using express mode*, page 51 or *Using advanced mode*, page 53 for more information.)

When you are adding content classifiers to a policy, you can select **Create Rule from Classifier** to add it manually. (See *Creating a rule from a content classifier*, page 99 for more information.)

When you are looking at a policy, you can click a rule in the tree view and select **Edit**, **New** > **Rule**, or **Delete**, or you can select these options from the toolbar.

Note that you cannot edit predefined content classifiers in the rules of the policy templates that Websense provides. On the Condition tab of these rules, you can view the name and type of predefined classifiers, but you cannot click links to view logic or change settings.

Rules can have one or more exceptions. To add an exception to a rule, click a rule in the tree view and select **New** > **Exception.** For information on adding exceptions, please see *Adding exceptions*.

Adding exceptions

Related topics:

- *Managing rules*, page 62
- *Adding a new exception*, page 63
- *Rearranging exceptions*, page 63

Most rules have exceptions.

In Websense Data Security, exceptions and rules are tightly linked, and exceptions are only triggered when rules are matched. If the rule is not matched, there is no need to apply exceptions to the rules.

There are a few ways to add an exception to a rule. On the **Main** tab under Policy Management, select Data Usage Policies or Data Discovery Policies.

- Click a rule and select **New** > **Exception** from the pull-down menu.
- Click a rule and select **New** > **Exception** from the toolbar.
- Click an exception and select **New** > **Exception Above** or **Exception Below**. This inserts the exception in an order of priority relative to others.

Like policies, exceptions have levels that define execution priority order. See *Rearranging exceptions*, page 63 for information on arranging exceptions.

Rearranging exceptions

Exceptions have execution priority order. The tree structure demonstrates the order that has been assigned, but you can change the order any time. When a policy is being applied, it applies exception 1 first, exception 2 second, and so on. If an exception is triggered, the next exceptions are not checked.

Manage the order of exceptions by choosing **More Actions** > **Rearrange Exceptions.** In the resulting box, highlight exceptions one by one and move them up or down in the priority sequence using the up and down arrows.

You can click an exception in the tree view and select **Rearrange Exceptions**. The same box appears.

Adding a new exception

Related topics:

- *Exception Wizard - General*, page 64
- *Exception Wizard - Properties*, page 65
- *Exception Wizard - Severity & Action*, page 66
- *Exception Wizard - Finish*, page 67

Exceptions are very much like rules. To add a new exception, click a rule in the policy tree view and select **New** > **Exception** or click an existing exception and select **New** > **Exception Above** or **Exception Below**.

The exception begins empty. You must select the fields to edit. The other fields retain the same data as the rule. There are 4 pages in the exception wizard:

- *General*
- *Properties*

- *Severity & Action*
- *Finish*

Complete the information on each page and click **Next** to proceed through the wizard.

Exception Wizard - General

Related topics:

- *Rule Wizard - General*, page 53

Field	Description
Policy name	The name of the affected policy.
Rule name	The rule related to this exception.
Exception name	Enter a name for this exception.
Description	Enter a description for this exception.

Exception Wizard - Properties

Related topics:

- *Rule Wizard - Source*, page 58
- *Rule Wizard - Destination*, page 59
- *Rule Wizard - Condition*, page 54

Field	Description
Exception Properties	In the left pane, highlight the property for which you want to make an exception and place a check mark next to it to enable it. ◆ **Condition** - Select **Condition** if you want to change the condition parameters established for the rule, such as the content classifier, threshold, or condition relations. ◆ **Source** - Select **Source** if you want to change the source of data defined for the rule. ◆ **Destination**- Select **Destination** if you want to change the destination of data defined for the rule.
Condition	Specify the exception you want to make for the rule’s condition. For example, if the rule is set to trigger when a PreciseID pattern is matched 10 times, but you want to raise the threshold for this exception, click the threshold and edit it here. See *Rule Wizard - Condition*, page 54 for explanations of the fields on this screen.
Source	Specify the exception you want to make for the rule’s source. For example, if a rule defined action plan A1 for all computers, but you want to execute A2 for laptops, click **Edit** and move laptops to the Exclude list. See *Rule Wizard - Source*, page 58 for explanations of the fields on this screen.
Destination	Specify the exception you want to make for the rule’s destination. For example, if the rule includes all destination channels, but you want a different action for the email channel, select Email here then edit the property. See *Rule Wizard - Destination*, page 59 for explanations of the fields on this screen.

Exception Wizard - Severity & Action

Related topics:

- *Rule Wizard - Severity & Action*, page 57

Field	Description
When the condition is matched, severity is:	Specify the severity of incidents that match this exception. This overrides the rule's severity: **Low** - Incidents that match this rule are of low importance. The policy breach is minor. **Medium** - Incidents that match this rule are of medium importance. The policy breach is moderate. **High** - Incidents that match this rule are very important and warrant immediate attention. The policy breach is severe.
and the action plan is	By definition, exceptions override the rule's action plan. Select an action for this exception. Note that action plans are customizable. By default, they include: ◆ **Block all** - Select this option if you want this policy to use the strict actions defined under **Main > Policy Management > Resources > Action Plans**. ◆ **Audit & notify manager** - Select this option (the default) if you want this policy to use the moderate actions defined. These are a compromise between the blocking and auditing plans. ◆ **Audit only** - Select this option if you want this policy to use audit incidents and not block them. Click the pencil icon to edit the action plan. You can change the action for each channel if desired. Editing an action plan changes it for all the rules and exceptions that use it. Click the paper icon to create a new action plan. See *Action Plans*, page 112, for details.

Field	Description
Advanced	This option does not apply the Web Security Gateway Anywhere customers. Click **Advanced** to define severity at a more granular level. For example, when there are more than 10 matches, change severity to medium and action plan to audit & notify. When there are more than 20 matches, change severity to high and action plan to block. Select a check box and define the parameters as needed.
Define Matches	This option does not apply the Web Security Gateway Anywhere customers. Select how matches should be calculated for this exception: ◆ **Greatest number of** matched conditions. Select this option if you want the number of matches for each condition to be compared, and only the greatest number reported. For example, if there are 5 matches for the condition, ConfidentialPattern, 3 for SSN_Pattern, and 10 for MyKeyPhrases, the number of matches would be defined as 10. ◆ **Sum of all** matched conditions. Select this option if you want the number of matches for each condition to be added together and the total to be reported. Given the same example as above, the number of matches would be defined as 18.

Exception Wizard - Finish

Click **Next** to display a summary of the exception you just created. You can go back to make changes or click **Finish** to accept them.

If you select **Finish**, the new exception is added to the policy you selected.

5 Classifying Content

When creating a policy, you use content classifiers to describe the data you are protecting. You can classify your content according to file properties, key phrases, and dictionaries, or you can fingerprint the data using Websense's patented PreciseID Fingerprinting technology.

To classify your content:

1. Select **Main** > **Policy Management** > **Content Classifiers**.
2. Select one of the content classifiers that are offered.

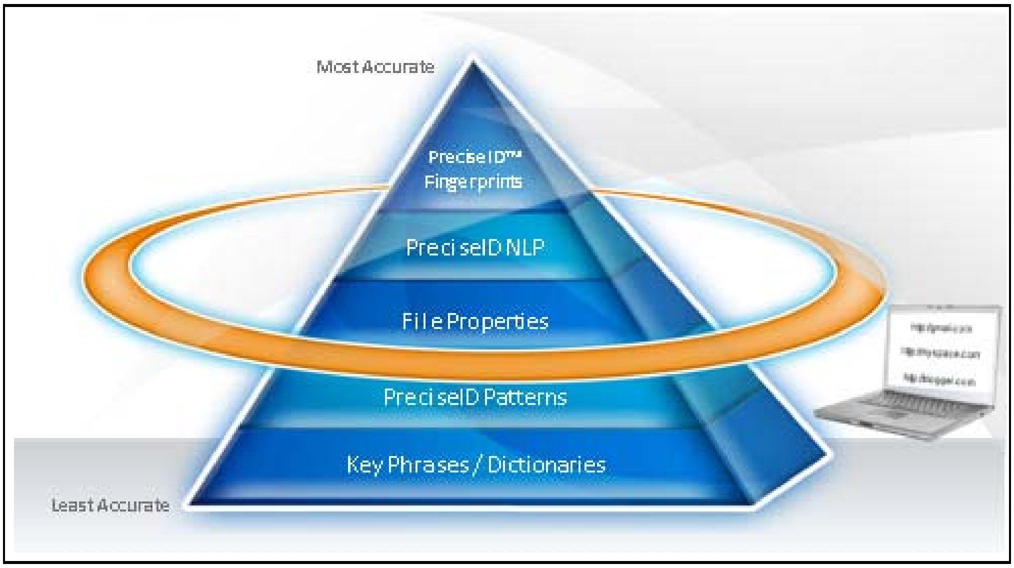
Classifier	Description
PreciseID Patterns	Lets you classify data by regular expression patterns. Used to identify alphanumeric strings of a certain format, such as 123-45-6789.
Key Phrases	Lets you classify data by the presence of a keyword or phrase, such as "confidential."
Dictionaries	Lets you classify data using terms that belong to a certain knowledge domain, such as medical or financial terms.
File properties	Lets you classify data by file name, type or size. File name identifies files by their extension. File type identifies files by metadata.
PreciseID Natural Language Processing (NLP)	Lets you classify data by context. Used for numeric data such as credit card numbers or intellectual property such as software design documents and source code.
PreciseID Fingerprinting - files & directories	Lets you fingerprint files or directories, including SharePoint directories.
PreciseID Fingerprinting - database records	Lets you fingerprint database records directly from your database or CSV file.

Websense provides predefined classifiers for the most common use cases. These are described in Appendix B: *Predefined Classifiers*, page 341. When classifying your content, you can select one of the predefined classifiers, customize a classifier to meet your needs, or create a new classifier from scratch.

Important

After you classify your content, you must add the content classifier to a rule and policy; otherwise, it has no effect. You are prompted to do this when you create a new classifier. Optionally, from the toolbar, you can select **Create Rule from Classifier**.

The diagram below illustrates the accuracy level of each content classifier. For the most accurate detection, use PreciseID fingerprint classifiers.



Once you classify your data, you create a rule containing the content classifier and the conditions in which content should be considered a match. For example, if the content contains 3 keywords and an attachment over 2 MB, trigger an incident. In the rule, you define the sources and destinations to analyze. Note that Data Security does not analyze all types of data. For example, it does not analyze the metadata of plain text files or the data inside Microsoft **.cab** files.

If you are going to create a database fingerprinting classifier, read *Preparing for fingerprinting*, page 90 and *Creating a validation script*, page 91. Websense Data Security automatically runs validation scripts on your new database fingerprinting classifiers if you set the scripts up properly.

Content classifier menu bar

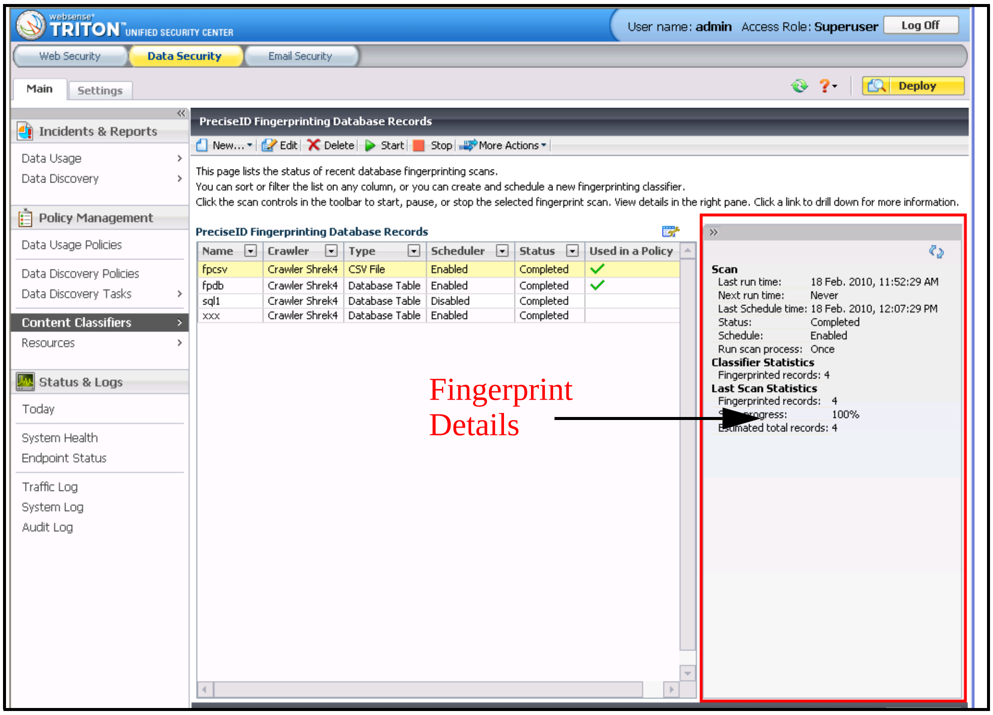
The following buttons are common to most classifiers:

Button	Icon	Description
New	🗋	Opens a dialog so you can create a new classifier of the selected type.
Delete	✕	Deletes the selected classifier. Be sure to check where the classifier's used before deleting it. (See **Where Used**, below.) **Note:** you can delete only one classifier at a time.
Create Rule from Classifier	📙	Creates a rule from the selected classifier and lets you mark it for use in an existing or new policy. **Note:** you can create a rule from only one classifier at a time. See *Creating a rule from a content classifier* for more details on this shortcut.
Where Used	?	Shows which policies, rules, and exceptions use this classifier.

The fingerprinting classifiers have additional menu options.

Button	Icon	Description
Start	▶	Starts fingerprinting. Begins the scan. Alerts that the task will be moved into manual mode.
Pause	⏸	Pauses fingerprinting.
Resume	⏯	Resumes fingerprinting.
Stop	■	Stops fingerprinting. Alerts that the task will be moved into manual mode.
More Actions	⇉	In addition to **Create Rule from Classifier** and **Where Used**, fingerprinting classifiers offer this option under More Actions: **Download Fingerprinting Report** - Database fingerprinting only. Downloads a detailed report on fingerprinting activities.

In addition, the fingerprinting classifiers offer a details pane on the right to show statistics about the scan and scheduler. See *Details pane*, page 72 for more information.



PreciseID Fingerprinting Database Records

This page lists the status of recent database fingerprinting scans.
You can sort or filter the list on any column, or you can create and schedule a new fingerprinting classifier.
Click the scan controls in the toolbar to start, pause, or stop the selected fingerprint scan. View details in the right pane. Click a link to drill down for more information.

PreciseID Fingerprinting Database Records

Name	Crawler	Type	Scheduler	Status	Used in a Policy
fpcsv	Crawler Shrek4	CSV File	Enabled	Completed	✓
fpdb	Crawler Shrek4	Database Table	Enabled	Completed	✓
sql1	Crawler Shrek4	Database Table	Disabled	Completed	
xxx	Crawler Shrek4	Database Table	Enabled	Completed	

Scan
Last run time: 18 Feb. 2010, 11:52:29 AM
Next run time: Never
Last Schedule time: 18 Feb. 2010, 12:07:29 PM
Status: Completed
Schedule: Enabled
Run scan process: Once
Classifier Statistics
Fingerprinted records: 4
Last Scan Statistics
Fingerprinted records: 4
Scan progress: 100%
Estimated total records: 4

Details pane

Fingerprinting classifiers offer a Details pane on the right to show statistics about the scan and scheduler. You can expand or collapse this pane to show more or fewer details. Click links, if offered, to see additional information on a particular statistic.

Scan

Statistic	Description
Last run time	The time and date of the last scan
Next run time	The next scheduled scan time
Last scheduled time	The last time a scan was scheduled
Status	The status of the scan. If the scan completed with errors, click the link to learn more details.
Schedule	Whether the schedule is enabled or disabled
Scan frequency	How often the scan is run

Task Statistics

Statistic	Description
Fingerprinted files/records	The total number of analyzed items
Fingerprint size	The total size of analyzed items
Endpoint package size	The size of the endpoint package
Used space on endpoint	The total amount of disk space used on the endpoint

Last Scan Statistics

Statistic	Description
Scanned files	The total number of items detected in the scan
Scanned size	The size of items detected in the scan, all totalled. (Does not apply to database scans.)
Scan/fingerprinting progress	The progress of the scan, in percentage completed
Fingerprinted files/records	The number of items sent to the policy engine's fingerprint repository.
Failed files	The number of items that failed for various reasons. Click the link to see more detail on failed items.
Filtered out files	The items that were not included by the filters you specified in the task definition. Click the link to see more detail on the items that were filtered-out.
Estimated total files/ records	An estimate of the total number of items
Estimated total size	An estimate of the total size of items
Fingerprinting rate	The speed at which the fingerprinting task was accomplished

PreciseID Patterns

Related topics:

- *Adding a PreciseID Pattern classifier*, page 75

To view or manage a list of content classifiers based on PreciseID patterns:

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **PreciseID Patterns**. Both user-defined and built-in patterns are shown. (These are distinguished by the icons in the Type column. You can sort the list by this column.)

Click **New** to add a new pattern classifier, **Delete** to delete the selected classifier, or **Where Used** to view where the classifier is used. The column, **Used in a Policy**, indicates whether the classifier is used in a policy at all.

Patterns can be detected within content (content includes the body of the content as well as any attachments). These patterns are regular expressions, such as Social Security numbers or credit card numbers that may appear in the content.

Setting a PreciseID Pattern enables you to define patterns to be searched for in content and to set what action should be taken when such a pattern is found. A basic PreciseID Pattern specifies a regular expression or a description of the pattern.

A regular expression is a string that is used to describe or match a set of strings, according to certain syntax rules. For example, the string “a\d+” matches all strings that start with the letter “a” and are followed by at least one digit, where “\d” represents any digit and “+” represents “at least one.” When the extracted text from a transaction is scanned, Websense Data Security uses regular expressions to find strings in the text that match patterns for confidential information. For example, this is a very basic regular expression for catching Visa credit card numbers:

```
\b(4\d{3}[\-\\]\d{4}[\-\\]\d{4}[\-\\]\d{4})\b
```

Because a regular expression file contains many internal attributes, if it is improperly written it can create many false-positive incidents intercepted on the system, can slow down Websense Data Security and impede analysis. If you are writing a regular expression to be used here, please contact Websense technical support for assistance.

One way of mitigating false positives in a pattern is to exclude certain values that falsely match it. When defining the classifier, you can define a *Pattern to exclude* listing words or phrases that are exceptions to the pattern rule (search for all Social Security numbers except these numbers that look like Social Security numbers but are not).

You can also add a *List of strings to exclude* listing words or phrases that, when found in combination with the pattern, affect whether or not the content is considered suspicious.

Another way to mitigate false positives is to consider the pattern as suspicious only when some other pattern or set of words appear in the analyzed data. To do this, you create another content classifier (a pattern, dictionary or any other), and combine the 2 in the condition of your rule with an AND operator.

When creating a rule for your policy, you can specify how many instances (matches) of the pattern must be found before the content is considered suspicious enough for the action to be taken (for example, 2 Social Security numbers seems reasonable, but 4 is already suspect). You do this on the **Condition** tab of the **Rule Properties** sheet.

For each content transmission, Websense Data Security tallies the number of instances in which the pattern was found in the content.

If the number of pattern matches is less than the number of matches set, the content is not considered suspicious and there is no further analysis.

If the number of pattern matches is equal to or greater than the number of matches set, the content triggers the action specified in the rule that uses this pattern.

Example:

The pattern is Social Security numbers and the number of matches is 4. The body of an email contains 3 Social Security numbers; the subject contains 2 Social Security numbers. Since there were 5 pattern matches, and this is greater than the number of set matches, the message triggers the action specified in the rule that uses this pattern.

When a pattern to exclude is added

You can define a list of exceptions to the pattern. This is a list of content that matches the pattern but should not be considered in the tally of pattern matches. For each content transmitted, Websense Data Security tallies the number of instances in which the pattern was found in the content, and subtracts the number of pattern-matches that are included in the Exclude list and compares this final number with the number of matches set.

Example:

The pattern is Social Security numbers, the number of matches is 2, and the list of excluded patterns is: 111-11-1111, 222-22-2222, and 333 33 3333 (total of three in the excluded list). The email contains 7 Social Security numbers: 111-11-1111, 222-33-4444, 444-55-6666, 555-66-7777, 222-22-2222, 777888-9999, 333-33-3333. The number of pattern matches is 7, minus 3 excluded patterns that were found in the email, thus equal to 4. Since 4 is greater than the number of matches (2), the message triggers the action specified in the rule that uses this pattern.

When a list of strings to exclude is added

You can add a String List that lists suspicious words to the PreciseID Patterns. When you do, for each content item transmitted, the action specified in the rule that uses this pattern is triggered only if the total number of pattern matches is above the number of matches and a word from the specified dictionary was found. If the number of matches is reached but no words from the dictionary are present, no further analysis is performed.

Example:

The pattern is Social Security numbers, the number of matches is 2, and the String List contains the phrases “Social Security” and “credit card.” The distributed content contains 3 Social Security numbers: 111-22-3333, 222-33-4444, 444-55-6666, but none of the words were found. Since the number of found distributed content (3) is greater than the number of matches (2), but there were no dictionary words in the email, no action is taken.

Adding a PreciseID Pattern classifier

There are 2 ways to add a new pattern classifier: you can create one from scratch, or you can base one on an existing classifier.

To create a pattern classifier from scratch:

1. Click **Main** > **Policy Management** > **Content Classifiers** > **PreciseID Patterns.** Click **New** from the menu bar.

   or

   While viewing a policy, select **New** > **Rule** > **Express mode** > **Help me create a new content classifier.** For Classifier type, select **PreciseID Patterns.**
2. Complete the fields as follows:

Field	Description
Name	Enter a name for this pattern, such as Visa card.
Description	Enter a description for this pattern, such as Visa credit card patterns.
Value	Enter the regular expression (RegEx) for which you want Websense Data Security to search, such as all 3-character strings followed by the sequence "123". The expression should be compatible with Perl syntax. Note that TRITON - Data Security does not validate your expression. Click the information icon for a list of valid values. To include unicode characters in your pattern, use the format \X{hex-number}.
Exclude	Click **Exclude** if you want to exclude certain values from the pattern, then select either **Pattern to exclude** or **List of strings to exclude** to define the pattern to exclude. Exclude should list exceptions to the rule. • **Pattern to exclude** - Define the regular expression pattern to exclude. Click the information icon for a list of valid values. • **List of strings to exclude** - Enter a list of phrases to exclude. Enter each phrase one by one, then click **Add** to add it to the list. These phrases, when found in combination with the pattern, affect whether the content is considered suspicious. Click **Remove** to remove selected phrases from the list.

3. Click **OK**.

To base a classifier on an existing classifier:

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **PreciseID Patterns**.
3. Click the classifier name that most closely resembles the classifier you want to create. Refer to *PreciseID patterns*, page 361 for details about each predefined classifier.
4. Change any of the fields you want to change or add or remove exclude values to those that are uneditable.
5. Click **Save As** at the top of the pane, then save the classifier under a new name.

   Note that you cannot edit a built-in pattern and save it under the same name. Built-in patterns are not editable.

⚠ **Warning**

If you customize one of Websense's built-in patterns and save it under another name, you are responsible for keeping that classifier up to date. Websense regularly updates classifiers with new regulations, but we cannot update a classifier that you have saved under a new name.

Key Phrases

Related topics:

- *Adding a key phrase classifier*, page 77

The presence of a keyword or phrase (such as "top secret" or "confidential") in content intended for an external recipient may indicate that classified information is being distributed. Websense Data Security enables you to block the distribution of this information by defining a key phrase classifier. No other protection features, such as fingerprinting, are required.

To view or manage a list of content classifiers based on key phrases:

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **Key Phrases**. Both user-defined and built-in patterns are shown. (These are distinguished by the icons in the Type column. You can sort the list by this column.)

Click **New** to add a new key phrase classifier, **Delete** to delete the selected classifier, or **Where Used** to view where the classifier is used. The column, **Used in a Policy**, indicates whether the classifier is used in a policy at all.

Adding a key phrase classifier

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **Key Phrases**.
3. Click **New** from the menu bar.
4. Complete the fields as follows:

Field	Description
Name	Enter a name for this key phrase classifier.

Field	Description
Description	Enter a description for this key phrase.
Phrase to search	Enter the key word or phrase that might indicate classified information. Key phrases are case-insensitive. White spaces are ignored, as are tags and metadata. Slashes, tabs, hyphens, underscores, and carriage returns are included in the search. Common words are also included, unlike when fingerprint scans are performed.

5. Click **OK**.

Dictionaries

Related topics:

◆ *Adding a dictionary classifier*, page 78

A dictionary is container for words and expressions belonging to the same language.

For your convenience, many dictionaries are built into Websense Data Security. There are lists for medical conditions, financial terms, legal terms, credit card terms, geographical locations, and more.

In Websense Data Security, you might create or customize a dictionary list that pertains to your line of business and then use this list in your policies, either as a classifier or an exception.

For example, in your policy, you might have a regular expression classifier that identifies all 13-digit numeric strings, and then use the credit card terms dictionary to further identify risk. This way you can remove false-positives.

To view or manage a list of content classifiers based on dictionaries:

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **Dictionaries**. Both user-defined and built-in patterns are shown. (These are distinguished by the icons in the Type column. You can sort the list by this column.)

Click **New** to add a new dictionary classifier, **Delete** to delete the selected classifier, or **Where Used** to view where the classifier is used. The column, **Used in a Policy**, indicates whether the classifier is used in a policy at all.

Adding a dictionary classifier

There are 2 ways to create a new dictionary classifier: you can create one from scratch, or you can base one on an existing classifier.

To create a dictionary classifier from scratch:

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **Dictionaries**.
3. Click **New** from the menu bar.
4. Complete the fields as follows:

Field	Description
Name	Enter a name for this pattern, such as Visa card.
Description	Enter a description for this dictionary, such as credit card terms.
List of phrases to include	Enter a word or phrase to include and click **Add**. Do this for each phrase to include until your list is complete. These phrases, when found in the content, affect whether the content is considered suspicious. (A match of any word in the dictionary triggers an incident.) White spaces are ignored, as are tags and metadata. Slashes, tabs, hyphens, underscores, and carriage returns are included in the search. Common words are also included, unlike when fingerprint scans are performed. Remove phrases by selecting them and clicking the **Remove** button.
The phrases in this dictionary are case-sensitive	Select this check box if you want the phrases that you entered to be added to the dictionary with the same case you applied.
Exclude	Click **Exclude** if you want to exclude certain values from the dictionary, then select either **Pattern to exclude** or **List of phrases to exclude**. Exclude should list exceptions to the rule. ◆ **Pattern to exclude** - Define the regular expression pattern to exclude. Click the information icon for a list of valid values. ◆ **List of phrases to exclude** - Enter a phrase to exclude and click **Add**. Do this for each phrase to exclude until your list is complete. Click **Remove** to remove selected phrases from the list.

5. Click **OK**.

To base one on an existing classifier:

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **Dictionaries**.
3. Click the classifier name that most closely resembles the classifier you want to create. Refer to *Dictionaries*, page 357 for details about each predefined dictionary classifier.
4. Change any of the fields you want to change. For example, add items to the phrase list. This lets you optimize your policy to compensate for false positives in your incident list.
5. Click **Save As**, then save the classifier under a new name.

   Note that you cannot edit a built-in dictionary and save it under the same name. Built-in patterns are encrypted and not editable.

File properties

Related topics:

- *Adding a file-type classifier*, page 80
- *Adding a file-name classifier*, page 81
- *Adding a file-size classifier*, page 81

Because classified data is often stored in specific file formats—such as PGP (encrypted) or Excel (xlsx)—Websense Data Security enables you to block the distribution of this information by defining file-type and file-name classifiers. You can also classify data by file size.

Tip

For a list of file types that the Websense Data Security supports, see *Supported File Formats*, page 367.

File-type classifiers group like files together. For example, office documents and pictures are 2 types of files. When you set up a file-type classifier, Websense Data Security examines the metadata in file headers traversing the system to determine the file type and act on it. You can create a new file type or add files and groups of files to the existing file types. (Refer to *File-type classifiers*, page 341 for details about each predefined file-type classifier.)

File-name classifiers identify files by file-name extension (such as *.docx) or the file name itself (such as myfile*.doc). Because end users can change the extension of files, this is a less secure means of identifying files.

File-size classifiers identify files by their size.

Adding a file-type classifier

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **File Properties**. Three tabs appear, with the **By Type** tab on top.
3. Click **New** from the menu bar.
4. Complete the fields as follows:

Field	Description
Name	Enter a name for this file type, such as “Picture Files.”
Description	Enter a description for this file type.

Field	Description
Filter by	The list of available file types is too long to appear in one window. In this field, enter criteria by which to filter the display. You can include wildcards if desired. “?” represents any single character, as in the example “file_?.txt”. “*” represents zero or more of any character, such as “*.txt”. Click the ▼ button to apply the filter.
Available file types	Select the file type(s) of interest in the left pane and click > to add it to this content classifier. The additions appear in the right pane. Scroll through the list of supported file types by clicking the video player controls above the list.

5. Click **OK**.

Adding a file-name classifier

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **File Properties**.
3. Click the tab, **By Name**.
4. Click **New** from the menu bar.
5. Complete the fields as follows:

Field	Description
Name	Enter a name for this group of files, such as “Report Files”.
Description	Enter a description for these files.
File names	Enter individual filenames to be protected, then click **Add**. You can use the “?” and “*” wildcards if desired. For example: *Report*.* To remove a file name from the list, select it and click **Remove**.

6. Click **OK**.

Adding a file-size classifier

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **File Properties**.
3. Click the tab, **By Size**.
4. Click **New** from the menu bar.

5. Complete the fields as follows:

Field	Description
Name	Enter a name for this group of files, such as “Medium Files” or “Large Files”.
Description	Enter a description for these files.
File size	Define the size of the files. - **At least** - Select this radio button if the file is always over a certain size, then specify the minimum size in KB. - **Between** - Select this radio button if the file is between 2 sizes, then specify the sizes in KB.

6. Click **OK**.

✓ **Note**

Some Websense components do not analyze files larger than certain threshold, for stability concerns. For discovery, endpoint removable media, and endpoint LAN control, Data Security performs file-size, file-name, and binary-fingerprint checks for files of unlimited sizes.

PreciseID Natural Language Processing (NLP)

Related topics:

- *Editing a PreciseID NLP classifier*, page 83

Websense Data Security provides a list of built-in PreciseID NLP classifiers that are written in a high-end development language that mimics natural language: Python. (See Appendix B*: Predefined Classifiers*.)

PreciseID NLP classifiers are most often used to classify numeric data such as credit card numbers and Social Security numbers. Because they are Python scripts optimized for this purpose, PreciseID NLP classifiers are more accurate than regular expression classifiers. PreciseID NLP scripts analyze both content and context using statistical analysis or decision trees.

Note that fingerprinting is better than NLP if you want to detect the exact credit card numbers in your database—for example, your customers’ credit card numbers.

If you care about credit cards in general, use the NLP classifier. NLP detects any valid credit card number. You may wish to use both with different levels of severity and different actions.

PreciseID NLP scripts can also be used to classify software design documents, source code (C, C++, C# and JAVA), SPICE, Verilog (Verilog hardware design source code), and VHDL (VHDL and VHDL AMS hardware design source code).

To view a list of content classifiers based on PreciseID NLP:

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **PreciseID Natural Language Processing**.

Click **Delete** to delete the selected classifier or **Where Used** to view where the classifier is used. The column, **Used in a Policy**, indicates whether the classifier is used in a policy at all.

You cannot generate your own PreciseID NLP scripts—there is no **New** button on this page—but you can edit one, change its parameters, and save it under a new name.

Click a classifier name to view or edit properties.

Be sure to add the classifier to a rule to activate it in your policy.

Upon request, Websense can create a custom classifier for your organization. Talk to your Sales Representative for more details.

Editing a PreciseID NLP classifier

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **PreciseID Natural Language Processing**.
3. Click the name of the classifier you want to edit.
4. Complete the fields as follows:

Field	Description
Name	The name of the predefined NLP classifier
Description	A description of the classifier
Edit parameter values	Select this check box if you want to edit the values of the script's parameters. Refer to *NLP scripts*, page 344 for details about the PreciseID NLP classifier you chose. Add a new value for each parameter as desired.
Exclude	Click **Exclude** if you want to exclude certain values from the classifier, then select either **Pattern to exclude** or **List of phrases to exclude** to define the pattern to exclude. Exclude should list exceptions to the rule. ◆ **Pattern to exclude** - Define the regular expression pattern to exclude. Click the information icon for a list of valid values. ◆ **List of phrases to exclude** - Enter a list of phrases to exclude, separated by commas. Click **Add** to add them to the list. These phrases, when found in combination with the script, affect whether the content is considered suspicious. Click **Remove** to remove selected strings from the list.

5. Click **OK** to save the edited script, or click **Save As** to save the edited classifier under a new name.

   If you click **Save As**, you are prompted to enter a new classifier name and description.

PreciseID Fingerprinting - files & directories

Related topics:

- *Managing Websense Data Security*, page 4
- *PreciseID Fingerprinting Wizard - General*, page 85
- *PreciseID Fingerprinting Wizard Shared Folder/Site Root*, page 85
- *PreciseID Fingerprinting Wizard - Scanned Files/Documents*, page 86
- *PreciseID Fingerprinting Wizard - Scheduler*, page 87
- *PreciseID Fingerprinting Wizard - File Filtering*, page 88
- *PreciseID Fingerprinting Wizard - Finish*, page 88
- *Classifying Content*, page 69

The presence of content intended for external recipients may indicate that classified information is being distributed via email and/or attachments. Websense Data Security enables you to block the distribution of this information by fingerprinting files and directories and scanning data in motion for those fingerprints.

Websense Data Security can protect SharePoint directories as well as any network file system or file shares.

To view or manage a PreciseID file or directory fingerprinting classifier:

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **PreciseID Fingerprinting - Files & Directories**. A fingerprint list appears. You can expand the right pane to view more details, such as last run time and next run time, or you can collapse it to show fewer. Click links in the details pane to learn more about the fingerprinted files and folders. You can also start, stop, or pause a fingerprinting task using buttons on the toolbar
3. To create a fingerprinting classifier click **New** > **File System Fingerprinting** or **New** > **SharePoint Fingerprinting** from the menu bar. A wizard opens. There are 6 pages in the wizard:
   - *General*
   - *Shared Folder (file system); Site Root (SharePoint)*
   - *Scanned Files (file system); Scanned Documents (SharePoint)*
   - *Scheduler*

- *File Filtering*
- *Finish*

Complete the information on each page and click **Next** to proceed through the wizard.

PreciseID Fingerprinting Wizard - General

Field	Description
Name	Enter a name for the documents you are fingerprinting, such as “finance documents.”
Description	Enter a description of this set of documents.
Crawler	The “crawler” is the agent that scans your documents looking for sensitive data. You can have several in your network if you are managing many documents. From the pull-down list, select which crawler to use to perform this fingerprinting. Typically this would be the crawler that is closest in proximity to the file folder or SharePoint site.
Fingerprinting Mode	Select which type of fingerprinting to perform: ◆ **Sensitive content** - Select this radio button to identify the content files and documents to fingerprint. ◆ **Ignored section** - Select this radio button to identify parts of secured documents that Websense Data Security should not analyze. This might include disclaimers, copyrights, and logos.
Fingerprinting Method	Select a fingerprinting method: ◆ **Content similarity** - Select this method to look for similarities between the scanned content and the file. This method provides greater security, because it detects sections of the document as well as exact file matches. ◆ **Exact match** - Select this method when you are only interested in exact matches. That is, when you only care if the scanned contents match the binary signature for the entire file. This method is quicker, but if someone edits just one character in the file, it is no longer detected. For large directory structures with many files, Websense recommends you initially set up an exact match classifier for immediate protection, then go back and change it to content similarity.

PreciseID Fingerprinting Wizard Shared Folder/Site Root

This page varies depending on whether you are defining a fingerprint for a file system or a SharePoint folder.

- *File system*, page 86
- *SharePoint*, page 86

When you click **Next** on this screen, the crawler tries to connect to the data source and notifies you of failure.

File system

Field	Description
Shared folder	Browse to the shared folder you want to scan.
User name	Enter a user name that has access to the shared folder.
Password	Enter the password for this user.
Confirm password	Enter the password again.
Domain (optional)	Optionally, enter the domain name of the user you entered above.

SharePoint

Field	Description
Site root	Browse to the site root you want to scan.
User name	Enter a user name that has access to the shared folder.
Password	Enter the password for this user.
Confirm password	Enter the password again.
Domain (optional)	Optionally, enter the domain name of the user you entered above.

When you click **Next** on this screen, Websense Data Security tries to connect to the folder/root-site using the given credentials. You are alerted if the attempt fails.

PreciseID Fingerprinting Wizard - Scanned Files/Documents

This page also varies depending on whether you are defining a fingerprint for a file system or a SharePoint folder.

- *File system*, page 86
- *SharePoint*, page 86

File system

Field	Description
Files and folders to scan	The files and folders included in and excluded from the scan are listed in the box. By default, nothing is included. Click **Edit** to modify the list. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool. Click the folder icon to display the directory one level up in the directory tree. You can also click the breadcrumbs above the list to navigate to another level.

SharePoint site

Field	Description
Documents to scan	The files and folders included in and excluded from the scan are listed in the box. By default, nothing is included. Click **Edit** to modify the list. Note that only the latest version of the documents is scanned, not the entire document history. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool. Click the folder icon to display the directory one level up in the directory tree. You can also click the breadcrumbs above the list to navigate to another level.

PreciseID Fingerprinting Wizard - Scheduler

Field	Description
Run scan	Select how often you want to run the scan process: once, daily, weekly, or continuously.
Hours to perform the scan	If you choose **Daily** or **Weekly**, specify the hours in which you want to run the scan, for example, daily at 2 a.m. Websense recommends you run fingerprint scans at night, after peak business hours.
But not before	If you select **Once** or **Continuously**, this check box appears. Select it if you want to run the scan as soon as possible, but not before a designated time or date. Then select a date from the pull-down box and a time from the spinner.
Wait xx minutes between consecutive scans	If you select **Continuously**, this option appears. Select a number from the spinner that represents the number of minutes to wait between consecutive scans.

PreciseID Fingerprinting Wizard - File Filtering

Field	Description
Filter by Type	
Include file types	List the types of files to be fingerprinted, separated by semi-colons. You can use the “*” or “?” wildcards. For example, “*.doc; *.xls; *.ppt; *.pdf”
Except	List the file types to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.
Filter by Age	
Search only for files that were modified:	Select this check box to filter files by age, then select the radio button that corresponds to the desired period. When you select this box, the default period is 24 months.
Filter by Size	
Scan only files larger than	Select this check box to filter files by size, then select a file size from the spinner. By default, all files larger than 1 KB are scanned.
Scan only files smaller than	Select this check box to filter files by size, then select a file size from the spinner. By default, all files smaller than 100,000 KB are scanned.

✓ **Note**

Files larger than 100 MB are fingerprinted only for exact-matching, regardless of this setting.

PreciseID Fingerprinting Wizard - Finish

A summary of this content classifier appears. It lists the name of the classifier, the crawler being used to perform the fingerprinting, the type of fingerprinting done, the shared directory, authentication information, the files and folders included and excluded, and the scan filters chosen. It also lists the schedule information.

When you click **Finish**, you’re prompted to add the classifier to a rule and policy. Continue with the wizard as prompted.

The actual fingerprint scan occurs according to its schedule.

PreciseID Fingerprinting - database records

Related topics:

- *Connecting to data sources*, page 89
- *Preparing for fingerprinting*, page 90
- *Creating a validation script*, page 91
- *Selecting the data to fingerprint*, page 92
- *How matches are counted*, page 94
- *PreciseID fingerprinting*, page 3
- *Creating a PreciseID database-record fingerprint classifier*, page 95
- *PreciseID Fingerprinting Wizard - General*, page 96
- *PreciseID Fingerprinting Wizard - Data Source*, page 96
- *PreciseID Fingerprinting Wizard - Field Selection*, page 97
- *PreciseID Fingerprinting Wizard - Scheduler*, page 98
- *PreciseID Fingerprinting Wizard - Fingerprinting Type*, page 98
- *PreciseID Fingerprinting Wizard - Finish*, page 98

Websense Data Security lets you quickly connect to a database, retrieve records, and fingerprint them. Websense Data Security uses PreciseID technology to detect exact fields from a protected database. For example, PreciseID can detect the first name, last name, and Social Security number occurring together in a message and corresponding to a specific record from the customer database.

In addition, Websense Data Security enables you to quickly import and fingerprint CSV files (UTF-8 encoded) that contain records.

You can also create a condition that combines record fingerprints and dictionary matches. A dictionary typically contains unique words or codes that are of classified nature, such as “Platinum,” “Gold,” “Silver,” and “Bronze.”

The presence of data and/or unique words or codes in content intended for external recipients may indicate that classified information is being distributed via email and/ or attachments. Websense Data Security enables you to block the distribution of this information by defining PreciseID record fingerprints.

Connecting to data sources

In order to fingerprint a database, the Data Security server must be able to connect to the data source over a supported interface. Websense Data Security supports the following database connection interfaces:

- Open Database Connectivity (ODBC)—Websense has certified support for the following ODBC-compliant databases:
  - Oracle 10g
  - Microsoft SQL Server 2008
  - Microsoft SQL Server Express
  - IBM DB2 9.5
  - IBM Informix IDS (IBM Informix ODBC driver 3.00.00.13223)
  - MySQL 5.1
  - Sybase ASE 15.0
- CSV files (UNC path needs to be specified: \\server\share\path_to_file.csv)

You can define flexible content policies for each data source. In each policy, you can configure detection rules by combining columns and indicating match thresholds.

✓ **Note**

Websense recommends that you test database connectivity before configuring content policies.

Preparing for fingerprinting

Before creating a database fingerprinting classifier, there are several steps you can take to streamline the process and optimize your results.This includes:

1. *Creating a Data Source Name (DSN) in Windows*
2. *Creating a validation script*
3. *Selecting the data to fingerprint*

Creating a Data Source Name (DSN) in Windows

When you are creating a database table fingerprint, you are prompted for DSN name. This is an ODBC term that refers to the name of the database to which you're connecting. If you have not already done so, you can create a DSN for your data source as follows:

1. Go to the crawler machine that you're using for fingerprinting tasks.
2. Select **Settings** from the Start menu, then select **Control Panel**.
   - On Windows NT systems, double-click the **ODBC Data Sources** icon.
   - On Windows XP systems, open the **Administrative Tools** folder and then double-click the **Data Sources (ODBC)** icon.
   - On some systems, the icon may appear labeled as "32bit ODBC."

   The ODBC Data Source Administrator appears with the **User DSN** tab selected. User DSNs are one of 3 types of DSNs managed by the ODBC Data Source Administrator:

- **User DSN**: The most common type of DSN. Stores information about how to connect to a specific data source. May be used only by the current user on the current machine.
- **System DSN**: Like the User DSN, the System DSN stores information about how to connect to a specific data source, but is available to all users on a particular machine, including NT services. Local to a computer, rather than dedicated to a user. The system, or any user having privileges, can use a data source set up with a system DSN. This is the preferred DSN type for Data Security.
- **File DSN**: Data Security does not support File DSNs.

3. Select the User DSN or System DSN tab and click **Add**. (You must be logged in as the Websense DSS Administrative User of the server running the relevant crawler to select the User DSN tab.)
4. From the Create New Data Source dialog box, select the driver for which you want to set up a DSN.
5. When prompted, enter a data source name and description. Depending on the driver you selected, you can enter more information. For Excel, select a workbook and enter the number of rows to scan. For Access, select the database and the page timeout.
6. Click **Advanced** or **Options** as needed to provide details on the database records you want to fingerprint, then click **OK**.

Creating a validation script

Fingerprinting columns with short field values can lead to multiple false-positive incidents. Websense Data Security includes a validation script that removes short alpha-numeric fields, small numbers, and values that should be ignored.

Many of our customers customize the validation script to validate their fingerprints. Others create validation scripts from scratch. Websense Data Security automatically runs scripts that are stored in a certain location and named a certain way.

During a fingerprinting scan, if the crawler finds a script matching the name of your fingerprinting classifier, it runs that script. If it does not, it searches for a default script and runs that. If neither exists, it does not perform validation.

If you would like to validate your fingerprinting scans, do the following:

1. Optionally, create a copy of the following files in the /validationScripts folder where Data Security was installed:
   - Validation.bat
   - Validation.py
   - Validation.xml

   If you prefer to create your script from scratch, you can skip this step.
2. Name your new validation script:

   ```
   <classifier-name>_validation.[bat|exe|py]
   ```

   And name your new configuration file:

`<classifier-name>_validation.[xml|ini]`
where <classifier-name> is the name you will assign the fingerprinting classifier.

Place both files in the /validationScripts folder on the server where the relevant crawler is installed.

3. The script should receive 2 command-line parameters: source file name and destination file name. It should read and perform validation on a csv-structure file (source) and write the validated results in a csv-structure file (destination).

   If you want to supply the script a third command-line parameter, use the configuration file for this purpose.

   The script should return a return code of 0 if everything succeeded, and non-zero if there was a problem.

4. The validation.xml configuration file that Websense provides contains the following parameters, which can be configured. If you write your own script, your configuration file can have any parameters.

   - <MinCharLength>: integer; minimal acceptable length for alphanumeric field (default: 4)
   - <MinNumber>: integer; minimal acceptable number (default: 10000)
   - <IgnoredDictionary>: string; path to UNICODE file containing [newline] delimited values to ignore in lower case in the UTF-16 encoding (default: <empty>)

5. Create and run the fingerprinting classifier with the given name.

During the scan, if the crawler finds a script named <classifier-name>_validation.[bat|exe|py], it runs that script. If it does not, it searches for a script named default_validation.[bat|exe|py] and runs that.

If the crawler receives a non-zero return code from the script, the fingerprinting process stops and an appropriate error is returned. In this case, you can either fix the script or remove it then refingerprint.

When Data Security finds a validation script, the Sample Data screen in the database fingerprinting wizard shows validated data, and not the raw data extracted from the database/CSV. (This is on the Field Selection page of the wizard, where you select **View Sample Data**.) You can use this to make sure that the validation script behaves as expected, and to see the exact information that is protected.

To run the script on subsequent fingerprint classifiers, copy the script and rename it.

Selecting the data to fingerprint

Fingerprinting is a powerful means of data monitoring and protection, but the processing can be time-consuming. For this reason, you should carefully consider what information you want to fingerprint.

When you are selecting the data to fingerprint, follow the rules below to achieve the right balance between optimal performance and accurate detection of your sensitive data

1. Avoid fingerprinting short values

Fingerprinting columns with short field values can lead to multiple false-positive incidents.

For numeric fields, we recommend that you fingerprint values with 5 digits and higher (>=10000) because:

- 4 digits easily match years (frequently appearing in email)
- 3 digits are quite common
- 1 and 2 digits numbers match days of month

The validation script template is a script that removes numbers with values less than the configured minimum (see *PreciseID Patterns*, page 73 for more details).

Note

If you must fingerprint a numeric column and removing numbers is not an option, please make sure that this column is always combined with another in the policy rule. For example, if it is an account number field, combine it with the Name, Address, or SSN of the person owning the account.

For non-numeric fields, we recommend that you fingerprint values with 4 or more characters. The reasoning is that:

- 3 letters are commonly used in abbreviations (TLA - Three Letters Abbreviation)
- 2 letters match U.S. states, country codes, etc.
- 1 letter has no real meaning

The validation script template removes non-numeric fields shorter than the configured length in characters.

Note

If you must fingerprint a non-numeric column and removing values is not an option, please make sure that this column is always combined with another in the policy rule. For example, if it is last name field, combine it with the first name, address or SSN of the person owning the account. Regardless, do NOT fingerprint fields shorter than 3 characters.

2. Avoid fingerprinting columns with repetitive values

Columns having repetitive values are quite common in databases. Fingerprinting such columns may cause performance issues both during the fingerprinting stage and real-time analysis. Fingerprinted repetitive fields may lead to large amounts of records matching analyzed transactions, and it will take time for the policy engine to go over the results.

For now, Websense recommends that you avoid fingerprinting columns with repetitive values. Many times, such columns have a very limited range of values, and they actually can be turned into a dictionary and attached to other policy rules in a PreciseID database policy.

3. Avoid fingerprinting uninteresting / irrelevant values

Some database tables / CSV files may contain values that should be ignored and excluded from fingerprinting. For example, a table may contain a value of 'N/A' instead of valid SSN. Looking through incidents (after the data was fingerprinted), you may locate additional candidates for ignoring.

The validation script template (described under *Creating a validation script*, page 91) allows you to ignore values that are specified in an external “ignored dictionary” file. If preferred, you can write your own scripts that filter any custom type of irrelevant data.

How matches are counted

In rules with a database fingerprinting classifier, the number of matches is defined as the number of records in the fingerprinted database that match the analyzed transaction. If a combination of phrases occurs more than once in the analyzed database, it does not account for more than 1 match.

For example, consider the following table:

Column_A	Column_B
1234	AAAA
5678	AAAA
1234	AAAA

And a condition specifying the combination of Column_A *and* Column_B.

- The text “1234 AAAA” produces a match count of 1. There are 2 records that consist of the match, but it appears only once in the text.
- The text “1234 AAAA 1234 AAAA” produces a match count of 2. Two records were fingerprinted, and 2 matches appear in the text.
- The text “AAAA 1234 5678” produces a match count of 2. Two records match, and the parts of text that match both records are not identical (although there’s only 1 match in the text for AAAA). This is because text may state “the following people have AAAA : 1234 and 5678”. Linguistically, this means AAAA applies to several records.
- The text “1234 AAAA 1234 AAAA 1234 AAAA” produces a match count of 2. Although there are several instances of the match, there are only 2 records (although duplicate) that are leaked.

The fingerprint repository itself generates high match-counts for duplicates. It adds a verification step that removes matches that don't match the logic above.

Creating a PreciseID database-record fingerprint classifier

Related topics:

- *PreciseID fingerprinting*, page 3
- *PreciseID Fingerprinting Wizard - General*, page 96
- *PreciseID Fingerprinting Wizard - Data Source*, page 96
- *PreciseID Fingerprinting Wizard - Field Selection*, page 97
- *PreciseID Fingerprinting Wizard - Scheduler*, page 98
- *PreciseID Fingerprinting Wizard - Fingerprinting Type*, page 98
- *PreciseID Fingerprinting Wizard - Finish*, page 98
- *Preparing for fingerprinting*, page 90

To create a PreciseID database-record fingerprinting classifier:

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **PreciseID Fingerprinting - Database Records**.
3. Click **New** from the menu bar then choose **Database Table Fingerprinting** or **CSV File Fingerprinting**. A wizard opens. There are 6 pages in the wizard:
   - *General*
   - *Data Source*
   - *Field Selection*
   - *Scheduler*
   - *Fingerprinting Type*
   - *Finish*

   Complete the information on each page and click **Next** to proceed through the wizard.

Important

The PreciseID fingerprinting technology uses data source names (DSNs) to perform database record fingerprinting. Before beginning the wizard, please use Windows control panel to create a DSN for the database records that you intend to fingerprint. See *Preparing for fingerprinting*, page 90 for instructions.

PreciseID Fingerprinting Wizard - General

Field	Description
Name	Enter a name for the database records you are fingerprinting, such as “finance records.”
Description	Enter a description for the database.
Crawler	From the pull-down list, select which crawler to use to perform this fingerprinting. (The “crawler” is the agent that scans your records looking for sensitive data.) Typically, you would select the crawler closest in proximity to the database server.

PreciseID Fingerprinting Wizard - Data Source

This screen varies depending on whether you are defining a fingerprint for a database table or a CSV file.

- *Database table*, page 96
- *CSV file*, page 97

When you click **Next** on this screen, the crawler tries to connect to the data source and notifies you of failure.

Database table

Field	Description
Data source name	Select the DSN for the database that you want to fingerprint. If you have not yet created a DSN for the database, please do so now or ask your database administrator to do so. (This is done in a Windows control panel.) See *Preparing for fingerprinting*, page 90 for instructions. Click refresh (⟳) to refresh the list. Note that this DSN must be defined on the Crawler you specified in the previous step.
Use data source credentials	Some DSNs allow you to save authentication credentials. Select this radio button if you set up credentials in the DSN, then you can use these credentials to provide access to the database records.
Use the following credentials	Select this radio button if you did not include authentication credentials in the DSN or if you want to override them. Then complete the fields as follows: • **User name** - Enter a user name that has access to the database. • **Password** - Enter the password for this user. • **Confirm password** - Enter the password again.

CSV file

Field	Description
User name	Enter a user name that has access to the CSV file.
Password	Enter the password for this user.
Domain	Optionally, enter the domain for this user.
CSV file name	Specify the path name of the CSV file to scan. For example: \\server-name\pathname\myData.csv

PreciseID Fingerprinting Wizard - Field Selection

Field	Description
Select fields from a table	Select this radio button if you want to select the fields to fingerprint from a list and see the resulting SQL query. If you select this button, do the following: 1. Select a table name from the drop-down list. (For Database Table only. For CSV files, the file is already selected.) 2. Select the field(s) you want to fingerprint. These correspond to columns in the table. 3. To change the displayed name of the field(s), click **Modify Displayed Names**, then edit the names as desired. (For Database Table only.) You can view the SQL query that was generated for your selection.This appears under **Selection as SQL Query**. Click **View Sample Data** to make sure that the correct information is fingerprinted.
Use the following SQL query to select records	Select this radio button if you want to generate your own SQL query. You can either type your own query or click **Copy Above Query** then modify it. Be sure to consult a database administrator when formatting the query, to make sure it doesn’t create any functionality, performance, or stability issues. Click **View Sample Data** to make sure that the correct information is fingerprinted. When you click **Next**, Websense Data Security validates your SQL query.

Tip

When you select the fields to fingerprint, be sure to follow the guidelines in *Selecting the data to fingerprint*, page 92. For example, avoid fingerprinting short values, columns with repetitive values, and uninteresting or irrelevant values.

PreciseID Fingerprinting Wizard - Scheduler

Field	Description
Run scan	Select how often you want to run the scan process: once, daily, weekly, or continuously.
Hours to perform the scan	If you choose **Daily** or **Weekly**, specify the hours in which you want to start the scan, for example, daily at 2 a.m. Websense recommends you run fingerprint scans at night, after peak business hours.
But not before	If you select **Once** or **Continuously**, this check box appears. Select it if you want to run the scan as soon as possible, but not before a designated time or date. Then select a date from the pull-down box and a time from the spinner.
Wait xx minutes between consecutive scans	If you select **Continuously**, this option appears. Select a number from the spinner that represents the number of minutes to wait between consecutive scans.

PreciseID Fingerprinting Wizard - Fingerprinting Type

Field	Description
Full fingerprinting	Select this radio button if you want a full scan to be performed every time your data is fingerprinted. (This could be a scheduled or on-demand fingerprinting task.) When you select this option, the entire chosen table is fingerprinted. These settings are changed on deploy. Whenever such a setting changes, both the changed repository and the primary repository become unsynchronized.
Differential fingerprinting	This option is much quicker. Select this radio button if you want Websense Data Security to fingerprint only records that have changed since the last scan, then select a field from the **Field by which to compare scans** list. The field you select should be one that changes incrementally every time a row is added—for example, a field named “seq_num” that increments by 1 with each addition. If this field has been updated since the last scan, Data Security remembers the last incremental change and resumes the scan from there. Because the data inside already-fingerprinted rows can change, you should run a full scan periodically. To do this, select the check box **Full scan every *nn* scheduled**

PreciseID Fingerprinting Wizard - Finish

A summary of this fingerprinting classifier appears. It lists the name of the data, the Crawler being used to perform the fingerprinting, the data source type, filename, and credentials. It also shows the SQL query and the fingerprinting type and schedule information.

When you click **Finish**, you’re prompted to add the classifier to a rule and policy. Continue with the wizard as prompted.

The actual fingerprint scan occurs according to its schedule.

Creating a rule from a content classifier

Related topics:

- *Classifying Content*, page 69

Field	Description
Content classifier	The content classifier from which you are creating a rule. This field is not editable.
Type	The type of content classifier: PreciseID Pattern, Key Phrase, etc. This field is not editable.
Rule name	By default, the name of this rule is the name of the classifier. Enter a new name if desired.
Add this rule to an existing policy	Select this radio button to add this rule to an existing policy. • **Policy Type** - Select the type of policy to which you want to add this rule: data usage or data discovery. • **Policy Name** - Select the exact policy to which you want to add this rule.
Add this rule to a new policy	Select this radio button to create a new policy for this rule. • **Policy Type** - Select the type of policy to create: data usage or data discovery. • **Policy Name** - Enter a name for the policy. • **Policy Description** - Enter a description for the policy. • **Policy level** - Select a policy priority level from the drop-down list. (Displayed only if the system has more than 1 level defined.) For more information, see *Policy levels*. • **Policy Owners** - Click **Edit** to select a policy owner or owners from a list.

6 Defining Resources

Related topics:

- *User directory entries*, page 103
- *Custom users*, page 104
- *Custom computers*, page 104
- *Networks*, page 105
- *Business Units*, page 106
- *Domains*, page 105
- *URL categories*, page 107
- *Printers*, page 108
- *Endpoint Devices*, page 109
- *Endpoint Applications*, page 109
- *Endpoint Application Groups*, page 110
- *Remediation scripts*, page 116
- *Action Plans*, page 112
- *Notifications*, page 119

In your policy, you can define the sources of and destinations for the data you want to protect. Depending on your subscription, you can also define the endpoint device or application that may be used, and the remediation action to take when a violation is discovered (such as block or notify). In Websense Data Security, these are known as *resources*.

Important

You do not have to define resources unless you want to tailor your policies for a small group. If you do not define resources, your policies and rules apply to all users, computers, networks, devices, etc. in your organization.

To define resources, click **Main** > **Policy Management** > **Resources**.

Resource	Description
Sources and Destinations	
User directory entries	Users or groups that may be a source or destination of sensitive data. These entries are imported from your user directory.
Custom users	Users not in your user directory who may be a source or destination of sensitive data.
Custom computers	Computers not in your user directory that may be a source or destination of sensitive data.
Networks	Networks that may be a source or destination of sensitive data.
Business Units	Business units that may be a source or destination of sensitive data.
Domains	Domains that may be a source or destination of sensitive data.
URL categories	URL categories that may be a source or destination of sensitive data.
*Printers**	Printers that may be a source or destination of sensitive data.
*Endpoint Devices**	Endpoint devices that may be the source or destination of sensitive data.
*Endpoint Applications**	Applications that may be a source or destination of your sensitive on endpoint machines.
*Endpoint Application Groups**	Application groups that may be a source or destination of sensitive data on endpoint machines.
Remediation	
Action Plans	The action to take when a breach is discovered.
*Remediation scripts**	The external script to run when a breach is discovered.
Notifications	The notification message to send when a breach is discovered, the person to send it to, and the format.

*Not included with Websense Web Security Gateway Anywhere

Sources and destinations

Related topics:

- *User directory entries*, page 103
- *Custom users*, page 104
- *Custom computers*, page 104
- *Networks*, page 105
- *Domains*, page 105
- *Business Units*, page 106
- *URL categories*, page 107
- *Printers*, page 108
- *Endpoint Devices*, page 109
- *Endpoint Applications*, page 109
- *Endpoint Application Groups*, page 110

There are many possible sources (origins) and destinations of information in your organization. Define them here, then in your policies' rules, specify which should be included or excluded.

User directory entries

Use this screen to view a list of users, groups, and computers that you imported from a user directory such as Microsoft Active Directory, Active Directory Application Mode (ADAM), or Lotus Domino. CSV files are also supported. These users, groups, and computers are possible sources or destinations of sensitive information in your organization.

There are likely too many users and groups to display on one screen. Use the **Search for** field to filter the display to just users and groups that meet certain criteria. You can enter free text or an asterisk (*) into this field. (Asterisk means search all.)

Use the **From type** field to select the type of entry to search for: computer, group, user, OU, or all.

Use the **In** field to select the specific directory server to search, or all servers.

Click **Apply** to apply the filter.

Use the radio controls to navigate from one screen to the next, or to the first or last.

Click the folder icon to display the directory one level up in the directory tree.

Note

Because this is a user directory import, you can view the list but not change or add anything.

Click **Settings** to add or set the order of user directory servers or initiate a user import.

Custom users

Use this screen to add or manage custom users—that is, users not part of the user directory service.

To add a custom user:

1. Click **New**.
2. Complete the fields as follows:

Field	Description
Name	Enter the name of the custom user.
Email address	Enter the email address for this person.
User name	Enter the person’s user name.
Windows NT domain	Optional. The domain name of the Windows NT domain for this user. ◆ Leave this field empty if the user doesn’t belong to a domain and should be considered a match when he logs onto his computer using a local account. ◆ Set this field to “*” if the user is part of a domain and should be considered a match for all domains. ◆ Set this field to a precise domain name if this user should be considered a match only when he or she logs onto this domain.
Title	Optional. Enter the person’s title.
Manager	Optional. Enter the name of the person’s manager.
Department	Optional. Enter the department to which this person belongs.
Phone number	Optional. Enter the person’s phone number.

3. Click **OK**.

Custom computers

Use this screen to view and set up a list of local computers that are possible sources or destinations of information in your organization, aside from the computers in the user directory.

To add a new computer to the system:

1. Click **New**.
2. Complete the fields as follows:

Field	Description
IP address or host name	Enter the IP address or host name for the computer.
FQDN	Enter a fully-qualified domain name for the computer (for example, myhost.example.com).
Description	Enter a description of this computer.

3. Click **OK**.

Networks

Use this screen to define the networks that are possible sources or destinations of sensitive information in your organization.

To add a network to the system:

1. Click **New**.
2. Complete the fields as follows:

Field	Description
Name	Enter a name for the network you are adding.
Description	Enter a description of this network.
Network address	Select this radio button to enter a network address and subnet mask for the network you are adding (for example, 255.255.255.0 is the subnet mask for the 192.168.1.0 network).
IP address range	Select this radio button to enter the IP address range for the network (for example, 192.168.0.0 to 192.168.255.255).

3. Click **OK**.

Domains

Use this screen to define the domains that are sources or destinations of information in your organization, typically for HTTP or FTP transactions. You can either block or permit everything that goes to these domains. For example, if your organization just acquired another company but you have not combined Active Directories yet, you may want to add the domain of the new company as an authorized destination.

To add a domain:

1. Click **New**.

2. Complete the fields as follows:

Field	Description
Domain	Enter name for this domain. You can enter a concrete domain name that is the name of a specific computer—like www.example.com. Or you can use wildcards that indicate a group of computers—for example, *.example.com, w*.example.com, www-?.example.com.
Description	Enter a description for this domain.

3. Click **OK**.

Business Units

Use this screen to set up a logical grouping of user directory entries (users, computers, networks, etc.) that may be a source or destination of information in your organization. A business unit is larger than a group but smaller than the company.

A business unit could comprise all the Marketing teams in your organization, regardless of their location.

When you create a business unit, you add users and computers to it. You can then assign it to a policy so that only these users and computers are permitted to send data of a particular type outside the company. If a business unit includes computers and users but a policy applies only to users, Websense Data Security applies the policy only to users in the business unit.

To define an organizational business unit:

1. Click **New**.
2. Complete the fields as follows:

Field	Description
Name	Enter name for this organization grouping or business unit.
Description	Enter a description for this business unit.
Display	From the drop-down list, select the user directory entry you want to add to the business unit: users, computers, etc. The entity you select then appears in the **Available List** grouping at the bottom of the screen.
Filter by	More users or groups may be available than can fit on one page. Use this field to specify criteria by which to filter the display, then click the **Apply filter** button.
Available list	Select the entities you want to add to the business unit and click the right arrow >. You can add an entire group and then use exclusions to remove people from the business unit. Use the video control buttons to view other pages in the list.

3. Click **OK**.

URL categories

Related topics:

- *Linking data and Web security*, page 226

If you are using Websense Web security solutions (Websense Web Security, Websense Web Security Gateway, or Websense Web Security Gateway Anywhere), use this screen to select the URL categories that may be the source or destination of sensitive information.

In your policies, you can use these categories to define rules for Web channels. For example, you may define a rule that credit card numbers cannot be posted to known fraud sites. (Please note that Data Security does not monitor URL categories on endpoint Web channels.)

To create a rule that uses URL categories this way:

1. Add a rule in advanced mode.
2. On the **Condition** tab, select the classifier of interest and set its threshold. For example, click **Add** > **PreciseID Pattern**, and choose a credit card classifier.
3. Set up the **Severity & Action** tab and **Source** tab as required for this rule.
4. On the **Destination** tab, select the **Web** check box, then click **Advanced** and select **HTTP/HTTPS**.
5. Click **Edit** and next to the **Display** field, choose **URL categories** from the drop-down list. Select the category of interest—for example, **Fraud**—and click > to add it to the include list.
6. Click **OK** and **Finish**.

URL categories are imported from the Websense category database. (You can view them, but you cannot change them.) Periodically click **Update Now** to reconnect with the database and update your category list.

Note that Websense Data Security supports predefined and custom categories. In your policy, you define whether these categories are authorized or unauthorized destinations of sensitive information.

Note that if you are using Websense Web Security Gateway or Web Security Gateway Anywhere, more than one category can be identified for a single URL: one for the static URL category—such as blogs— and one for the dynamic content, such as gambling if the blog is about gambling. Websense Web Security looks up static URL categories and the gateway module analyzes dynamic content. Both categories are reflected in your incident reports.

> **Important**
>
> To take advantage of Websense URL categories, you must configure linking and enable the Websense Linking Service. See *Linking data and Web security*, page 226 for more information.

Printers

If you have installed a printer agent, this screen displays the printers that it monitors. Each printer is associated by a name, type (auto-detected or user-defined), and print server (IP address or host name).

Initially, only printers that were detected by the printer agent are shown.

If desired, you can add printers to the list, such as printers that are connected to an endpoint device (requires an endpoint agent).

To add a printer:

1. Click **New** in the toolbar.
2. Complete the fields as follows:

Field	Description
Name	Enter a name for the printer you're adding.
Description	Enter a description for this printer.
IP address or host name	Enter the IP address or host name of the print server managing this printer.

3. Click **OK**.

In your policy, you can define whether to permit or block sensitive information from going to these printer destinations.

> **Note**
>
> If you have Websense Web Security Gateway Anywhere, this section does not apply to you.

Endpoint Devices

✓ **Note**

This section applies only to customers with the endpoint agent known as Websense Data Endpoint. If you have Websense Web Security Gateway Anywhere, it does not apply to you.

Use this screen to define the endpoint devices that you want to cover your policies. If you do not define devices, all devices are covered.

To add a device:

1. Click **New**.
2. Complete the fields as follows:

Field	Description
Name	Enter name for this type of device, such as “R&D devices”
Description	Enter a description for this type of device.
Value	Enter a specific device name. You can use wildcards, if desired. For example: K*320 Value should be an exact device name if you are not using wildcards.

3. Click **OK**.

Endpoint Applications

✓ **Note**

This section applies only to customers with the endpoint agent known as Websense Data Endpoint. If you have Websense Web Security Gateway Anywhere, it does not apply to you.

Websense provides a long list of built-in applications that you can choose to monitor on the endpoint when you set up your endpoint policy. These applications, including Web applications and SaaS (software as a service) applications, are included in Appendix D, *Endpoint Applications*.

If there are endpoint applications that you want to cover that are not on our list, use this screen to define those applications.

To add an application:

1. Click **New** > **Application** or **New** > **Online Application**.

2. Complete the fields as follows:

Field	Description
Name	Enter name for this application, such as Microsoft Word.
Executable file	Enter the executable name for this application, such as “winword.exe”.
Description	Enter a description for this application.
Belongs to	Select this check box to associate the application with an existing application group, then select the group of interest.
Trusted application	Select **Trusted Application** to indicate that Websense Data Security does not need to enforce this application. Trusted applications are permitted to write any type of information to removable media.
Screen capture	From the pull-down list, select the action to take for screen capture operations performed using this application. You can block and audit, permit and audit, or permit screen captures.

3. Click **OK**.

Note that our built-in applications are identified by the application metadata. This is a very secure method of identifying application usage.

When you add applications using this screen, they are identified by their executable name. Occasionally, users try to get around being monitored by changing the executable name. For example, if you’re monitoring “winword.exe” on users’ endpoint devices, they may change the executable name to “win-word.exe” to avoid being monitored.

If you want to add an application so that it is identified according to the application metadata, you must use an external utility program.

For information on the utility and instructions on using it, see *Importing other applications*, page 382.

Endpoint Application Groups

✓ **Note**

This section applies only to customers with the endpoint agent known as Websense Data Endpoint. If you have Websense Web Security Gateway Anywhere, it does not apply to you.

Websense provides a list of application groups that group applications in like categories. Below are the default application groups and the operations allowed on them.

Type	Copy/Cut	File Access	Paste	Download
Packaging Software		X		
P2P		X	X	
Office Applications	X			
IM		X	X	
FTP		X	X	
Encryption Software		X		
Email		X	X	
Device Control		X		
CD Burners		X		
Browsers	X	X	X	

Use the following screen to define application groups that are not on our list.

1. Click **New > Application Group** or **New > Online Application Group.** Applications include software packages like Microsoft Word and Excel that you install locally. Online applications are those accessed over the Web.
2. Complete the fields as follows:

Field	Description
Name	Enter a name for the application group, such as Desktop Publishing.
Description	Enter a description for the application group.
Members	Click **Edit** to select applications to include in this group. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool.
Endpoint operations	Select the operations to be analyzed in any application in the group. For example, click Cut/copy to analyze all Cut and Copy operations performed in one of the applications.

3. Click **OK**.

Remediation

Related topics:

- *Remediation scripts*, page 116
- *Action Plans*, page 112
- *Notifications*, page 119

Once you've defined which information can go where, you can define what remediation to perform when a policy breach is discovered.

Action Plans

Related topics:

- *Remediation scripts*, page 116
- *Adding a new action plan*, page 113
- *Notifications*, page 119

Use this page to define the plan of action to take when various breaches are discovered. Two action plans are provided by default.

Name	Description
Block all	This action plan is designed for severe breaches. It blocks all activity on all channels. It requires a subscription to Websense Data Protect.
Audit only	This action plan, the default, is designed for mild breaches. It permits all activity on all channels and logs incidents in the audit log.

✓ **Note**

The predefined action plans use the Default notification. You can edit the action plans to use a different notification—see *Notifications*, page 119 and *Adding a new message template*, page 119 for details.

When you add rules to a policy, you select the action plan to use.

To create a new action plan, click **New**. To delete an action plan, select it and click **Delete**.

When you have all your action plans configured, select the one to use by default. To do so, select the plan, then click **Set as Default Action Plan**.

Adding a new action plan

The procedure for adding an action plan varies depending on your subscription. You may see:

- *Standard options*
- *Web Security Gateway Anywhere mode*

Standard options

1. Click **New**.
2. Enter an action plan name and description.
3. On the **Data Usage** tab, complete the fields as follows:

Field	Description
Email	Select an action to take when a breach is discovered on an email channel.
FTP	Select an action to take when a breach is discovered over FTP.
Chat	Select an action to take when a breach is discovered over chat.
HTTP/HTTPS	Select an action to take when a breach is discovered on HTTP or HTTPS channels.
Plain text	Select an action to take when a breach is discovered via plain text.
Network printing	Select an action to take when a breach is discovered on a network printer.
Endpoint HTTP/ HTTPS	Select an action to take when a breach is discovered on an endpoint device over HTTP or HTTPS.
Endpoint application	Select an action to take when a breach is discovered on an endpoint application such as Word.
Endpoint removable media	Select an action to take when a breach is discovered on an endpoint device such as a thumb drive.
Endpoint LAN	Select an action to take when a breach is discovered on an endpoint LAN, such as when a user copies sensitive data from a workstation to a laptop.
Endpoint printing	Select an action to take when a breach is discovered on a local or network printer that is connected to an endpoint.

Field	Description
Audit incident	Select this check box if you want Websense Data Security to log incidents in the incident database. When you choose a block action, this check box is enabled by default. **Note:** If you disable this box, incidents are not logged, so you will not know when a policy is breached. When **Audit incident** is enabled, several more options are made available. You can: • Run remediation script • Run endpoint remediation script • Send syslog message • Send email notifications
Run remediation script	Select this check box if you want Websense Data Security to run a remediation script when an incident is discovered, then select the script to use from the pull-down list. See *Remediation scripts*, page 116 for more information.
Run endpoint remediation script	Select this check box if you want Websense Data Security to run an endpoint remediation script when an incident is discovered, then select the script to use from the pull-down list.
Send syslog message	Select this check box if you want to notify an outside syslog server or ticketing system of the incident.
Send email notifications	Select this check box to send an email message to a designated recipient when a policy is breached. Select the message or messages to send. Click a link to view or modify standard messages. Click **New** to create a custom message. See *Notifications*, page 119 and *Adding a new message template*, page 119 for details. **Tip**: There is a benefit to using the same template for each action plan. Data Security gathers notifications for individual users according to templates and combines them into a single notification. So if an incident contains 10 different rules, each with a different action plan but the same template, the user receives a single notification with the details of all the breaches.

The actions available for each channel depend on the the channel. Possible actions include:

Action	Description
Permit	Let the message through.
Block	Deny or block the message.
Quarantine	Quarantine the message.
Quarantine and encrypt on release	Quarantine the message. Encrypt it if and when it is released.

Action	Description
Encrypt	Encrypt the message.
Confirm	Display a confirmation message, such as “Are you sure you want to do this?”

4. If you subscribe to Websense Data Discover, click the **Data Discovery** tab and complete the fields as follows:

Field	Description
Audit	Select this check box if you want Websense Data Security to log data discovery incidents in the audit log.
Run remediation script	Select this check box if you want Websense Data Security to run a remediation script when an incident is discovered, then select the script to use from the pull-down list. See *Remediation scripts*, page 116 for more information.
Run endpoint remediation script	Select this check box if you want Websense Data Security to run an endpoint remediation script when an incident is discovered, then select the script to use from the pull-down list.

5. Click **OK** to save your changes.

Web Security Gateway Anywhere mode

1. Click **New**.
2. Enter an action plan name and description.
3. Complete the remaining fields as follows:

Field	Description
Action	Select the action to take when a user is breaching policy: ◆ **Permit** - Allow the HTTP, HTTPS, or FTP request to go through. ◆ **Block** - Block the request.

Field	Description
Audit incident	Select this check box if you want Websense Data Security to log incidents in the audit log. When the audit log is enabled, you can also send email notifications.
Send email notifications	Select this check box to send an email message to a designated recipient when a policy is breached. Select the message or messages to send. Click a link to view or modify standard messages. Click **New** to create a custom message. See *Notifications*, page 119 and *Adding a new message template*, page 119 for details. **Tip**: There is a benefit to using the same template for each action plan. Data Security gathers notifications for individual users according to templates and combines them into a single notification. So if an incident contains 10 different rules, each with a different action plan but the same template, the user receives a single notification with the details of all the breaches.

4. Click **OK** to save your changes.

Remediation scripts

Related topics:

- *Adding a new remediation script*, page 117
- *XML interface*, page 118

Use this screen (**Resources** > **Remediation Scripts**) to define an external script to run when various breaches are discovered.

✓ **Note**

If you have Websense Web Security Gateway Anywhere, this section does not apply to you.

⚠ **Warning**

To avoid degrading system performance, it is highly recommended you consult with Technical Support before adding a remediation script.

There are 3 types of remediation scripts:

- **Endpoint Script -** used for endpoint incidents. When a breach is discovered on an endpoint, this script is run automatically. Because the script is run on an endpoint device, it should have minimal CPU and disk space requirements. In addition, it should not assume the endpoint computer is part of the network.

- **Incident Management Script -** this script is not executed automatically. To activate this script, you open an incident under **Main** > **Incidents & Reports**, then click **Remediate** > **Run Remediation Script** on the menu bar and select which script to run on that incident.
- **Policy Script -** used for data usage and discovery incidents. When a breach is discovered on a usage or discovery transaction, this script is run automatically. Because it's associated with the network server, it can be larger and more demanding of CPU resources, and it can be based on other tools in network.

All 3 of these commands are configured the same way. For policy scripts, however, you'll notice 2 tabs: Windows and Linux. This enables you to add separate commands for Windows and Linux operating environments.

Adding a new remediation script

1. Click **New** then select the type of command to create from the menu.
2. Complete the fields as follows:

Field	Description
Name	Enter name for this external command.
Description	Enter a description for this command
Executable file	Browse to the executable file you want to run. To change your selection, right-click **Browse** and select a new file.
Arguments (optional)	Optionally, enter any arguments you want to include with the command. If the arguments are enclosed in quotation marks, separate arguments by a space. For example: "-e" "-o"
Additional Files	If the script requires additional files, such as a resource file or other scripts that it calls, click **Additional Files** then browse to a zip file containing the additional file(s) to run. **Note:** Additional files are placed in the same folder as the the script, and they are automatically downloaded by the endpoints.
User name	Enter the user name to impersonate when logging onto the machine to access the script.when it is time to execute it.
Password	Enter the password for this user.
Domain (optional)	Optionally, enter the domain name of the machine.

3. Click **OK**. A progress bar shows the progress of each file as it uploads. You can cancel the process at any time. When the upload is complete, the new external command appears in the details pane.

When editing an existing script, you'll see **Update** buttons instead of **Browse** buttons. To edit a script:

1. Click the script name to edit.

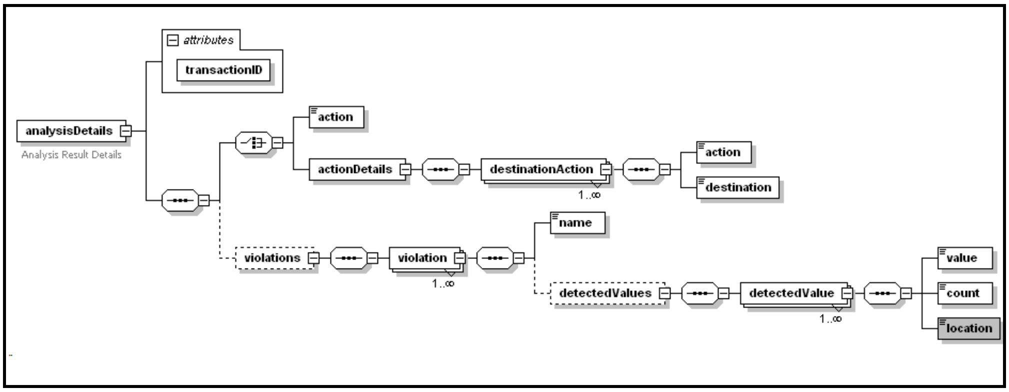
2. By **Current executable file**, click **Update**. You are alerted that the executable file will be removed from the Data Security Management Server.
3. Click **OK** to continue.
4. Browse to the new executable file.
5. If necessary, update the additional files in the same way.
6. Click **OK**.

XML interface

Websense Data Security creates an XML file every time an incident is generated. The XML file contains incident details that your script can use, such as the nature of the violation and the content itself.

At run time, your script receives the path to the XML file as an input. Your script can parse this XML file and perform addition actions based on the incident details, such as logging to an external system or custom analysis.

The XML Schema Definition (XSD) for this file is shown below:



Where:

Element	Description
analysisDetails	Root element.
transactionID	The internal transaction ID (unique ID that Websense Data Security generates for every analyzed transaction).
action	The action taken (for example, permit or deny).
actionDetails	The action taken per destination.
violations	The detected violations, including the policy name and content.
name	Descriptive policy name
detectedValues	The matched sensitive content and its location (for example, email body or file attachment).

Notifications

Related topics:

- *Adding a new message template*, page 119

Use this screen to define whom to notify when a breach is discovered. Websense Data Security offers a built-in notification template, **Default notification**, that you can edit as required.

Click a message name to see its contents and define its recipients.You can use the default notification, delete it, or create a new template.

Data Security gathers notifications for individual users according to templates and combines them into a single notification. So if an incident contains 10 different rules, each with a different action plan but the same template, the user receives a single notification with the details of all the breaches.

On the other hand, if there is only one breach and the action plan includes 2 different notification templates, the user would receive 2 separate notifications, assuming he's a member of both recipient lists.

Adding a new message template

1. Select **Main** > **Policy Management** > **Resources**.
2. From the Remediation section, select the **Notifications** option.
3. Click **New** on the toolbar.
4. Enter a name and description for this notification template, such as "Breach notification".
5. On the **General** tab, complete the fields as follows:

Field	Description
Sender name	Enter the name of the person from whom notifications should be sent. This is the name that will appear in the email **From** field. Maximum length: 1024 characters.
Sender email address	Enter the email address of the person from whom notifications should be sent. Maximum length: 1024 characters.

6. The outgoing mail server that's been configured appears on screen. If you want to change the server used, click **Edit** (the pencil icon).

7. Complete the remaining fields as follows:

Field	Description
Subject	Type the subject of the notification. This appears in the email **Subject:** line. Click the right arrow to choose variables to include in the subject, such as "This is to notify you that your message was %Action Taken% because it breached corporate policy." Maximum length: 4000 characters.
Recipients	Define the recipient(s) for the notification. Click **Edit** to select to select business units or directory entries. Select **Additional email addresses** then click the right arrow to select a dynamic recipient that varies according to the incident. For example, you can choose to send the notification to the policy owners, administrators, source, or source's manager. Select the variable that applies, such as %Policy Owners%. Separate multiple addresses with commas.

8. On the **Notification Body** tab, select a notification type and display format from the drop-down lists.

Field	Description
Type	Select the type of notification to send: ◆ **Standard** - Select **Standard** to include all of the elements shown in the Body Content box. You can enable or disable these elements if you use the standard notification type. ◆ **Custom** - Select this option if you want to send a custom notification. Edit the default text as needed. The drop-down menu provides variables.
Display as	Select a display format from the drop-down list: HTML or plain text.
Logo	Displays the Websense logo, date, and time.
Action	Displays the action taken when the breach was discovered.
Message to user	Displays a message in the message body. You can use the default text, or edit it to your liking. The drop-down menu provides variables.
Incident details	Displays incident details in the notification message.
Violated rules	Attaches a list of rules violated by the breach.

Field	Description
Allow users to release blocked email	This option does not apply to Web Security Gateway Anywhere customers. Select this check box if you want to allow users to release blocked messages by replying to their notification message. If you do not have the Exchange agent, you must configure a Websense mailbox to activate this capability. Refer to the *Knowledge Base* article titled “Configuring the Force Mailbox” for details.
Attach policy-breach content	Attaches policy breach contents to the email message.

9. Click the **Notification Design** button to preview your message.
10. Click **OK** to save your changes.

7 Performing Discovery

Related topics:

- *Creating a data discovery policy*, page 124
- *Scheduling Data Discovery Tasks*, page 135
- *Configuring discovery incidents*, page 131
- *Viewing discovery status*, page 130
- *Viewing discovery results*, page 131
- *Updating discovery*, page 131
- *Copying, moving, or encrypting discovered files*, page 132

✓ **Note**

This chapter applies only to customers with Websense Data Discover. It does not apply those with Websense Web Security Gateway Anywhere.

Discovery is the act of determining where sensitive content is located in your enterprise. A data discovery policy might say, for instance: every Sunday, scan all the computers in the network looking for financial documents containing the keyword “Confidential”. Log what is discovered and send a notification to the Finance manager.

If you want to monitor what is done with those financial records or stop them from leaving the building, you need to create a network or endpoint policy.

Discovery enables you to find data at rest on your network and identify the endpoint machines that represent the greatest risk. This allows you to prioritize actions taken on the files and machines.

Performing discovery is comprised of 2 basic steps:

1. *Creating a data discovery policy*, page 124
2. *Scheduling Data Discovery Tasks*, page 135

Structurally, data discovery policies are the same as data usage policies. Both are comprised of rules, exceptions, content classifiers, and resources. Rather than specifying destination channels to scan such as FTP, SMTP, and printers, however, you create a data discovery task that describes where and when to perform the discovery, including specific network and endpoint computers to scan.

On networks, this may include a file system, SharePoint directory, database, or Exchange server.

- File systems - Scans your network file systems and identifies data in breach of policies.
- SharePoint - Scans SharePoint directories and identifies data in breach of policies.
- Database - Scans the organization’s database servers and detects confidential information that is defined as policy breaches in tables.
- Exchange - Scans the organization’s Exchange servers and detects confidential information that is defined as policy breaches in mailboxes and public folders.

If you’re performing endpoint discovery, it includes the exact devices to scan.

Data discovery policies are different from data usage policies in other subtle ways as well. For example, you tend to classify content differently in database discovery than you do on Web channels.

In addition, a false positives or false negatives in discovery are typically less troubling, because the information is not being sent out of the organization.

Creating a data discovery policy

Related topics:

- *Scheduling Data Discovery Tasks*, page 135
- *Creating a custom policy*, page 49
- *Managing rules*, page 62
- *Adding exceptions*, page 62
- *Using express mode*, page 51
- *Using advanced mode*, page 53

1. Select **Main** > **Policy Management** > **Data Discovery Policies.**
    a. If you have not already selected policies from the built-in regulatory template list, you’re prompted to do so. Click **Next** and select the base policies to apply in your discovery.
    b. Highlight a policy to read details about it. You can view all relevant policies or only those that are commonly used. (For more information about these regulatory compliance policies, refer to *Predefined Policies*, page 317.)

c. Select the policies you want to apply in your organization by checking the box next to their policy names. When you are satisfied with the policies you have selected, click **Next**.

d. The **Finish** screen appears, summarizing your selections. Click **Finish**. The Websense Data Security policy database is updated and a confirmation message appears.

2. In the toolbar, click **New** > **Policy**.

3. Complete the fields as follows:

Field	Description
Policy name	Enter a name for this policy.
Enabled	Select this check box to enable the policy in your organization.
Description	Optionally, provide a description of this policy.
Policy owners	By default, no policy owners are included in the policy. To define a policy owner(s), click **Edit**. In the resulting box, select the people who should receive notification in the event of a policy breach. Click the right-arrow to move them into the Selected List. These are known as *policy owners*. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool.

4. Click **OK**. The Create a Rule dialog box appears, because all policies must contain at least one rule to function. (Policies can be free of rules, but they will have no system effect.)

5. Indicate whether you want to use express or advanced mode to create the rule. Express mode handles most of your needs.

Field	Description
Express mode	Select this mode if you want to accept the default rule properties for your data. See *Using express mode*.
Advanced mode	Select this if you want to specify rule properties using a wizard. See *Using advanced mode*.
I don’t want to create a rule now	Select this if you want to create a rule later. you can add one any time by highlighting a policy and clicking New Rule.

Like data usage policies, you can add rules and exceptions to data discovery policies. The procedure is the same. See *Managing rules*, page 62 and *Adding exceptions*, page 62 for instructions.

Scheduling the scan

Related topics:

- *Scheduling Data Discovery Tasks*, page 135
- *Performing file system discovery*, page 126
- *Performing SharePoint discovery*, page 127
- *Performing database discovery*, page 128
- *Performing Exchange discovery*, page 129
- *Performing endpoint discovery*, page 130

Once you create a data discovery policy, you need to schedule the scan. Select **Main > Policy Management > Data Discovery Tasks** to do this. You can schedule network discovery tasks or endpoint discovery tasks.

For more information, see *Scheduling Data Discovery Tasks*, page 135.

Performing file system discovery

Related topics:

- *Scheduling Data Discovery Tasks*, page 135
- *Creating a data discovery policy*, page 124
- *Scheduling network discovery tasks*, page 138
- *File System tasks*, page 138

To perform discovery on a network file system:

1. Create a data discovery policy. (See *Creating a data discovery policy*, page 124 for instructions.)
2. Select **Main > Policy Management > Data Discovery Tasks**.
3. Select **Network Tasks**.
4. Click **New > File System Task** on the toolbar.
5. Complete the fields on the screen and click **Next** to proceed through a wizard. For details on each screen, see the sections below:
   a. *File System Discovery Task Wizard - General*, page 139
   b. *File System Discovery Task Wizard - Networks*, page 139
   c. *File System Discovery Task Wizard - Scanned Folders*, page 140
   d. *File System Discovery Task Wizard - Scheduler*, page 141

    e. *File System Discovery Task Wizard - Policies*, page 141
    f. *File System Discovery Task Wizard - File Filtering*, page 141
    g. *File System Discovery Task Wizard - Advanced*, page 143
    h. *File System Discovery Task Wizard - Finish*, page 143
6. Deploy your changes by clicking **Yes** when prompted.
7. Discovery will take place at the time and day you scheduled in step 5d. To start it immediately, click **Switch to Mode** > **Manual**, then click **Start** > **Full Scan**. A message indicates when the scan finishes.
8. To view and respond to discovery results, click **Main** > **Incidents & Reports** > **Data Discovery**. See *Viewing the incident list*, page 175 for information on reading these screens.

Performing SharePoint discovery

Related topics:

- *Scheduling Data Discovery Tasks*, page 135
- *Creating a data discovery policy*, page 124
- *Scheduling network discovery tasks*, page 138
- *SharePoint tasks*, page 143

To perform discovery on SharePoint folders:

1. Create a data discovery policy. (See *Creating a data discovery policy*, page 124 for instructions.)
2. Select **Main** > **Policy Management** > **Data Discovery Tasks**.
3. Select **Network Tasks**.
4. Click **New** > **SharePoint Task** on the toolbar.
5. Complete the fields on the screen and click **Next** to proceed through a wizard. For details on each screen, see the sections below:
    a. *SharePoint Discovery Task Wizard - General*, page 144
    b. *SharePoint Discovery Task Wizard - Scanned Site*, page 144
    c. *SharePoint Discovery Task Wizard - Sites*, page 144
    d. *SharePoint Discovery Task Wizard - Scheduler*, page 144
    e. *SharePoint Discovery Task Wizard - Policies*, page 146
    f. *SharePoint Discovery Task Wizard - File Filtering*, page 146
    g. *SharePoint Discovery Task Wizard - Advanced*, page 147
    h. *SharePoint Discovery Task Wizard - Finish*, page 147
6. Deploy your changes by clicking **Yes** when prompted.

7. Discovery will take place at the time and day you scheduled in step 5d. To start it immediately, click **Switch to Mode** > **Manual**, then click **Start** > **Full Scan**. A message indicates when the scan finishes.
8. To view and respond to discovery results, click **Main** > **Incidents & Reports** > **Data Discovery**. See *Viewing the incident list*, page 175 for information on reading these screens.

Performing database discovery

Related topics:

- *Scheduling Data Discovery Tasks*, page 135
- *Creating a data discovery policy*, page 124
- *Scheduling network discovery tasks*, page 138
- *Database tasks*, page 147

To perform discovery on a database:

1. Create a data discovery policy. (See *Creating a data discovery policy*, page 124 for instructions.)
2. Select **Main** > **Policy Management** > **Data Discovery Tasks**.
3. Select **Network Tasks**.
4. Click **New** > **Database Task** on the toolbar.
5. Complete the fields on the screen and click **Next** to proceed through a wizard. For details on each screen, see the sections below:
   a. *Database Discovery Task Wizard - General*, page 148
   b. *Database Discovery Task Wizard - Data Source Name*, page 148
   c. *Database Discovery Task Wizard - Scheduler*, page 148
   d. *Database Discovery Task Wizard - Policies*, page 149
   e. *Database Discovery Task Wizard - Table Filtering*, page 149
   f. *Database Discovery Task Wizard - Advanced*, page 150
   g. *Database Task Wizard - Finish*, page 150
6. Deploy your changes by clicking **Yes** when prompted.
7. Discovery will take place at the time and day you scheduled in step 5c. To start it immediately, click **Switch to Mode** > **Manual**, then click **Start** > **Full Scan**. A message indicates when the scan finishes.
8. To view and respond to discovery results, click **Main** > **Incidents & Reports** > **Data Discovery**. See *Viewing the incident list*, page 175 for information on reading these screens.

Performing Exchange discovery

Related topics:

- ◆ *Scheduling Data Discovery Tasks*, page 135
- ◆ *Creating a data discovery policy*, page 124
- ◆ *Scheduling network discovery tasks*, page 138
- ◆ *Exchange tasks*, page 150

To perform discovery on email on a Microsoft Exchange server:

1. Create a data discovery policy. (See *Creating a data discovery policy*, page 124 for instructions.)
2. Select **Main** > **Policy Management** > **Data Discovery Tasks**.
3. Select **Network Tasks**.
4. Click **New** > **Exchange Task** on the toolbar.
5. Complete the fields on the screen and click **Next** to proceed through a wizard. For details on each screen, see the sections below:
    a. *Exchange Discovery Task Wizard - General*, page 151
    b. *Exchange Discovery Task Wizard - Mailboxes & Folders*, page 152
    c. *Exchange Discovery Task Wizard - Exchange Servers*, page 151
    d. *Exchange Discovery Task Wizard - Scheduler*, page 153
    e. *Exchange Discovery Task Wizard - Policies*, page 153
    f. *Exchange Discovery Task Wizard - File Filtering*, page 154
    g. *Exchange Discovery Task Wizard - Advanced*, page 154
    h. *Exchange Discovery Task Wizard - Finish*, page 155
6. Deploy your changes by clicking **Yes** when prompted.
7. Discovery will take place at the time and day you scheduled in step 5d. To start it immediately, click **Switch to Mode** > **Manual**, then click **Start** > **Full Scan**. A message indicates when the scan finishes.
8. To view and respond to discovery results, click **Main** > **Incidents & Reports** > **Data Discovery**. See *Viewing the incident list*, page 175 for information on reading these screens.

Performing endpoint discovery

Related topics:

- *Scheduling Data Discovery Tasks*, page 135
- *Creating a data discovery policy*, page 124
- *Scheduling endpoint discovery tasks*, page 155

To perform discovery on endpoint systems:

1. Create a data discovery policy. (See *Creating a data discovery policy*, page 124 for instructions.)
2. Select **Main** > **Policy Management** > **Data Discovery Tasks**.
3. Select **Endpoint Tasks**.
4. Click **New** on the toolbar.
5. Complete the fields on the screen and click **Next** to proceed through a wizard. For details on each screen, see the sections below:
   a. *Endpoint Discovery Task Wizard - General*, page 156
   b. *Endpoint Discovery Task Wizard - Endpoints*, page 156
   c. *Endpoint Discovery Task Wizard - Scheduler*, page 156
   d. *Endpoint Discovery Task Wizard - Policies*, page 156
   e. *Endpoint Discovery Task Wizard - File Filtering*, page 157
   f. *Endpoint Discovery Task Wizard - Advanced*, page 157
   g. *Endpoint Discovery Task Wizard - Finish*, page 158
6. Deploy your changes by clicking **Yes** when prompted.
7. Discovery will take place at the time and day you scheduled in step 5c. To start it immediately, click **Switch to Mode** > **Manual**, then click **Start** > **Full Scan**. A message indicates when the scan finishes.
8. To view and respond to discovery results, click **Main** > **Incidents & Reports** > **Data Discovery**. See *Viewing the incident list*, page 175 for information on reading these screens.

Viewing discovery status

To view the status of a data usage discovery task:

1. Select **Main** > **Policy Management** > **Data Discovery Tasks**.
2. Select **Network Tasks**.
3. View the **Status** column of the task list table.

You can sort, group, or filter by the **Status** column. You can view further statistics in the **Details** pane on the right of the screen.

You cannot view the status of endpoint discovery.

Viewing discovery results

To view and respond to discovery results, click **Main** > **Incidents & Reports** > **Data Discovery**. You can view the data discovery report catalog or the incident list. The report catalog lists reports into the discovery incident database. The incident list lists all data discovery incidents and their details.

See *The report catalog*, page 161 and *Viewing the incident list*, page 175 for information on reading these screens.

You can also look at the **Today** page (**Main** > **Status & Logs** > **Today**). This page includes a summary of data discovery incidents, including the top 5 hosts and top 5 policies per incident. It also lists the date and time the last data discovery incident was received.

Updating discovery

Running subsequent data discovery tasks on already discovered networks updates the information in the system, finding new violations.

To update a data discovery task, double-click the data discovery task under **Main** > **Policy Management** > **Data Discovery Tasks** modify the schedule (or switch the mode to manual and click **Start** to update immediately).

You cannot edit a task while it is running.

Configuring discovery incidents

You can configure the number of incidents to display in the Incidents & Reports section for discovery:

1. Select **Settings** > **System** > **Incidents & Reports**.
2. Select the **Data Discovery Incidents** tab.
3. Complete the fields as described in *Setting preferences for data discovery incidents*, page 212.

Copying, moving, or encrypting discovered files

If you want, you can copy, move, or encrypt sensitive content (files) when it's discovered. For this purpose, Websense Data Security includes the following remediation scripts.

- **CopyFiles -** Copies files that are in breach of corporate policy to another directory. Within the CopyFiles script file, users can define to ignore files that have not been accessed in X number of days.
- **MovesFiles -** Moves (not copies) files that are in breach of corporate policy to another directory for quarantine. In the original location, the file is replaced with a text message: "This file was detected to contain content that is a breach of corporate policy and thus has been quarantined. For more information please contact your system administrator". Within the MoveFiles script file, users can define to ignore files that have not been accessed in X number of days.

Preparing and running the remediation scripts

Edit the script files:

1. Open the scripts in Notepad. By default, they're located in the RunCommands directory where Websense Data Security is installed.
2. Edit the scripts as follows:

   CopyFiles - Define the destination of the copied files in the "Location" field. For example: Location = r'\\127.0.0.1\quarantine_copy'. Location should be a network share accessible to all servers running discovery.

   MovesFiles - Define the destination of the moved files in the "Location" field. For example: Location = r'\\127.0.0.1\quarantine'

   - DaysKeepActiveFiles - Number of days to keep files parameter.
   - QuarentineMsg - Message to place in the stubbed file.

Configure the scripts:

1. Select **Main** > **Policy Management** > **Resources** > **Remediation Scripts**.
2. Select **New** > **Incident Management Script**.
3. Enter a name and description for these data discovery scripts.
4. Browse to the executable file of interest: **CopyFiles.py or MoveFiles.py**. By default, they're located in the RunCommands directory where Websense Data Security is installed.
5. Enter a user name and password for an administrator that has: read permissions to the archive folder, access to all directories in the network, and read/write privileges to all files scanned in the discovery.
6. Click **OK**.

Add the remediation scripts to an action plan:

1. Select **Main** > **Policy Management** > **Resources** > **Action Plans**.

2. Select an action plan or select **New** from the toolbar.
3. Select the check box **Run remediation script**, and select the script to run.
4. Click **OK**.

Add the action plan to a policy:

1. Select **Main** > **Policy Management** > **Data Discovery Policies**.
2. Select the rule of interest and click **Edit**.
3. Navigate to the **Severity & Action** page.
4. Select the action plan.
5. Click **OK**

Deploy your changes.

The remediation script will run when data discovery incidents are triggered on the selected policy.

✓ **Note**

Keep in mind: The users that you define in the User Credentials above should be users that:

- Are administrators with access privileges to all directories in the network.
- Have read/write privileges to all files that are scanned by the discovery process

If remediation scripts will access shares that are under a Active Directory domain, the Data Security server must be part of the domain as well.

8 Scheduling Data Discovery Tasks

Related topics:

- *Scheduling network discovery tasks*, page 138
- *Scheduling endpoint discovery tasks*, page 155
- *File System tasks*, page 138
- *SharePoint tasks*, page 143
- *Database tasks*, page 147
- *Exchange tasks*, page 150

✓ **Note**

This chapter applies only to customers with Websense Data Discover. It does not apply those with Websense Web Security Gateway Anywhere.

There are 2 types of data discovery tasks:

- Network discovery tasks - used to set up discovery on network file systems, shared (SharePoint) directories, databases, and Exchange servers.
- Endpoint discovery tasks - used to set up discovery on endpoint hosts.

To configure a data discovery task:

1. Select **Main** > **Policy Management** > **Data Discovery Tasks**.
2. Select **Network Tasks** or **Endpoint Tasks**. A list of existing tasks displays.

Sorting and filtering tasks

You can sort, group, and filter tasks by the column name. Click the down arrow by any column name and choose an option:

Field	Description
Sort Ascending	Select this option to sort the table by the active column in ascending alphabetical order.
Sort Descending	Select this option to sort the table by the active column in descending alphabetical order.
Filter by (column)	Select this option to filter the data in the table by the type of information in the active column, such as by description or task name.
Clear filter	Select this option to clear the filter and display all tasks.

Buttons and controls

All data discovery tasks have these options:

Button	Icon	Description
New	🗋	Creates a new data discovery task.
Edit	✏	Lets you edit the active data discovery task. If your changes require deployment, the task changes to **Stopped (deployment needed)** status. When restarted, task starts from the beginning.
Delete	✕	Deletes the active data discovery task.

In addition, network discovery tasks have scan controls and other options. These are very similar to the fingerprinting scan controls.

Button	Icon	Description
Start	▶	Starts a discovery scan.
Stop	■	Stops a discovery scan. When restarted, task starts from the beginning.
Pause	⏸	Pauses a discovery scan. When restarted, task starts from the last point it was paused.
Download Discovery Report	⭳	Downloads a detailed report on discovery scanning activities in CSV format.

Details pane

Network tasks also offer a Details pane on the right to show statistics about the scan and scheduler. You can expand or collapse this pane to show more or fewer details.

Scan

Statistic	Description
Last run time	The time and date of the last scan.
Next run time	The next scheduled scan time.
Last scheduled time	The last time a scan was scheduled.
Status	The status of the scan. If the scan completed with errors, click the link to learn more details.
Schedule	Whether the schedule is enabled or disabled.
Scan frequency	How often the scan is run.

Task Statistics

Statistic	Description
Scanned items/tables/files	The total number of analyzed items.
Scanned size	The total size of analyzed items in MB.
Scanned mailboxes/ records/computers/shares	Total number of analyzed mailboxes, records, computers, or shares (depending on the type of scan).

Last Scan Statistics

Statistic	Description
Scanned items/tables/files	The total number of items detected in the scan.
Scanned size	The size of items detected in the scan in MB, all totaled. (Does not apply to database scans.)
Scan progress	The progress of the scan, in percentage completed.
Analyzed items/tables/files	The number of items sent to the policy engine’s fingerprint repository.
Failed items/tables/files	The number of items that failed for various reasons. Click the link to see more detail on failed items.
Filtered out items/tables/ files	The items that were not included by the filters you specified in the task definition. Click the link to see more detail on the items that were filtered-out.
Scanned mailboxes/ records/computers/shares	The total number of mailboxes that were scanned.
Estimated total items/ tables/files/records	An estimate of the total number of items.

Last Scan Statistics

Statistic	Description
Total records/items to scan	The number of records you've chosen, out of the total, to scan.
Estimated total size	An estimate of the total size of items in MB.

Scheduling network discovery tasks

Related topics:

- *File System tasks*, page 138
- *SharePoint tasks*, page 143
- *Database tasks*, page 147
- *Exchange tasks*, page 150

Select **Policy Management > Data Discovery Tasks > Network Tasks** to configure discovery on your network machines. The resulting screen displays all of the network discovery tasks that have been established to date.

Note that network discovery is performed on a host name if it is supplied, an FQDN if there is no host name, and an IP address if there is no host name or FQDN. The crawler does not search all of these, only the first property it encounters.

There are 4 types of network tasks:

- *File System tasks*
- *SharePoint tasks*
- *Database tasks*
- *Exchange tasks*

To add a new network task, click **New** then select the type of task to create from the menu: file system, SharePoint, database, or Exchange. A wizard appears.

File System tasks

The wizard for creating file system discovery tasks has 8 pages:

- *File System Discovery Task Wizard - General*
- *File System Discovery Task Wizard - Networks*
- *File System Discovery Task Wizard - Scanned Folders*
- *File System Discovery Task Wizard - Scheduler*
- *File System Discovery Task Wizard - Policies*

- *File System Discovery Task Wizard - File Filtering*
- *File System Discovery Task Wizard - Advanced*
- *File System Discovery Task Wizard - Finish*

File System Discovery Task Wizard - General

Field	Description
Name	Enter a name for this discovery task.
Description	Enter a description for this discovery task.
Crawler	Select the crawler to perform the scan. Typically, this is the crawler that is located in closest proximity to the network server.

File System Discovery Task Wizard - Networks

Field	Description
Edit	By default, discovery runs on no computers or networks. Click **Edit** to select the computers and networks to scan. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool.
Advanced	Click **Advanced** if your network uses a port other than the default Windows port—for example, if you have a Linux/UNIX NFS server or a Novell file server. Enter the port number(s) your network uses. Separate multiple entries by commas.

Note

If you choose network objects larger than 65536 potential addresses (larger than a class C subnet), you are warned and prompted to confirm.

File System Discovery Task Wizard - Scanned Folders

Field	Description
Scanned folders	Select the shared folders you want to scan: ◆ **Administrative shares** - Select this if you want to scan administrative share drives (sometimes known as hidden shares) such as C$ and D$. ◆ **Shared folders** - Select this if you want to scan shared folders such as PublicDocs. ◆ **Specific folders** - Select this if you want to scan specific folders, then enter the name(s) of the folder(s) to scan, separated by semi-colons.
Scan method	Select the method of port scanning to use when scanning network shares: ◆ **TCP** - Select TCP if you want to scan the share drives using transmission control protocol. ◆ **ICMP** - Select ICMP if you want to scan the share drives using Internet control message protocol. ICMP is faster than TCP, however, ICMP may trigger firewall alerts. (The behavior of scanning for open shares using ICMP is similar to what viruses do.) If you want to use ICMP, configure your firewall to ignore the specific server running the crawler.
User name	Enter the user name of any user with network access to the specified computer/shares.
Password	Enter and confirm a password for this administrator.
Domain	Optionally, enter the domain name of the network.

⚠ **Warning**

The network administrator credentials aren't verified at this point until the scan starts. If you enter the wrong credentials here, authorization fails later. Be careful to enter a valid user name and password.

File System Discovery Task Wizard - Scheduler

Field	Description
Enabled	Select this check box to enable the scheduler for the current task. Deselect **Enabled** to gain manual control over the task. When the scheduler is disabled, you can start and stop tasks using the scan controls on the toolbar.
Run scan	Select how often you want to run the scan process: once, daily, weekly, or continuously. Continuously means that the crawler restarts after every scan, operating continuously. (You can set the wait interval.)
Hours to perform the scan	If you choose **Daily** or **Weekly**, specify the hours in which you want to run the scan, for example, daily at 2 a.m.
But not before	If you select **Once** or **Continuously**, this check box appears. Select it if you want to run the scan as soon as possible, but not before a designated time or date. Then select a date from the pull-down box and a time from the spinner.
Wait xx minutes between consecutive scans	If you select **Continuously**, this option appears. Select the number of minutes to wait between consecutive scans. (Each scan starts from the beginning.)

File System Discovery Task Wizard - Policies

Field	Description
All discovery policies	Select this radio button if you want all discovery policies to be applied in this scan. Websense Data Security will search for data that matches the rules in all deployed policies
Selected policies	Select this radio button if you want only certain policies to be applied in this scan, then select the policies to apply.

File System Discovery Task Wizard - File Filtering

Field	Description
Filter by Type	Select this check box if you want to filter the files to scan by file type, then indicate what file types to include in the scan and what exceptions to make, if any.
Include file types	List the types of files to be scanned, separated by semi-colons. You can use the “*” or “?” wildcards. For example, “*.doc; *.xls; *.ppt; *.pdf” Click **File Types** to select the file types to include by extension. You can add or edit file types in the resulting box if necessary. To set Data Security to scan all files, set **Include file types** to *. You can also filter by name: for example, all the files which have the word *temp*: “*temp*.*”

Field	Description
Except	List the file types to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.
Filter by Age	Select this check box if you want to filter the files to scan by file age. Then select one of the following radio buttons:
Scan only files that were modified:	• **Within** - Select this button if you want to search only for files that were modified within a certain period, then indicate the period (in months) using the spinner. • **More than** - Select this button if you want to search only for files that were modified more than a certain number of months ago, then specify the number using the spinner. • **Between** - Select this button if you want to search for files modified between 2 dates, and specify the dates.
Filter by Size	Select this check box if you want to filter the files to scan by file size. You can select one or both of the check boxes. If you select both, you are specifying a range to scan.—for example, files larger than 5 MB but smaller than 100 MB.
Scan only files larger than	Select this box to scan only files *larger* than a certain size, then use the spinner to specify the size.
Scan only files smaller than	Select this box to scan only files *smaller* than a certain size, then use the spinner to specify the size.

✓ **Note**

Network discovery has a limit of 255 characters for the path and file name. Files contained in paths that have more than 255 characters are not scanned.

File System Discovery Task Wizard - Advanced

Field	Description
No limit	Select this radio button if you do not want to limit the bandwidth used for the discovery process.
An average of (1-9999) Mbps	Select this radio button if want to limit the bandwidth used for the discovery process to an average number of megabytes per second, then select the desired limit. This prevents strain on your file servers, network adapters, and on the Websense Data Security system.
Full scan schedule	Select one of the following radio buttons to indicate when you want to perform full discovery scans: ◆ **Only on policy update** - Select this option if you want to perform full discovery only when a discovery policy changes. ◆ **On policy update or fingerprinting version update** - Select this option if you want to perform full discovery when a discovery policy *or* a fingerprinting version changes. ◆ **Always** - Select this option if you want to perform full discovery on the scheduled time no matter what has changed. (We don’t recommend choosing “always,” because this slows the discovery process and taxes the system and file servers.)
File access timestamp	Select **Preserve original access time** if do not want Websense Data Security to alter the timestamp on files it scans. By default, it updates the “Last Accessed” timestamp of each file it scans. **Note:** To preserve access time, you must give Data Security read-write privileges for all hosts where discovery is being performed.

File System Discovery Task Wizard - Finish

Displays a summary of the file system discovery task you just established.

SharePoint tasks

The wizard for creating SharePoint discovery tasks has 8 pages:

- *SharePoint Discovery Task Wizard - General*
- *SharePoint Discovery Task Wizard - Scanned Site*
- *SharePoint Discovery Task Wizard - Sites*
- *SharePoint Discovery Task Wizard - Scheduler*
- *SharePoint Discovery Task Wizard - Policies*
- *SharePoint Discovery Task Wizard - File Filtering*
- *SharePoint Discovery Task Wizard - Advanced*
- *SharePoint Discovery Task Wizard - Finish*

SharePoint Discovery Task Wizard - General

Field	Description
Name	Enter a name for this discovery task.
Description	Enter a description for this discovery task.
Crawler	Select the crawler to perform the scan. Typically, this is the crawler that is located in closest proximity to the SharePoint server.

SharePoint Discovery Task Wizard - Scanned Site

Field	Description
Site Root	Address of the SharePoint site root. For example: http://192.168.10.2/shared/.
User name	Enter the user name of a user with access to the SharePoint.
Password	Enter and confirm a password for this user.
Domain	Optionally, enter the domain name of the network.

SharePoint Discovery Task Wizard - Sites

Field	Description
Edit	By default, discovery runs on no SharePoint sites. Click **Edit** to select the SharePoint sites to scan. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool.

SharePoint Discovery Task Wizard - Scheduler

Field	Description
Enabled	Select this check box to enable the scheduler for the current task. Deselect **Enabled** to gain manual control over the task. When the scheduler is disabled, you can start and stop tasks using the scan controls on the toolbar.
Run scan	Select how often you want to run the scan process: once, daily, weekly, or continuously.
Hours to perform the scan	If you choose **Daily** or **Weekly**, specify the hours in which you want to run the scan, for example, daily at 2 a.m.

Field	Description
But not before	If you select **Once** or **Continuously**, this check box appears. Select it if you want to run the scan as soon as possible, but not before a designated time or date. Then select a date from the pull-down box and a time from the spinner.
Wait xx minutes between consecutive scans	If you select **Continuously**, this option appears. Select a number from the spinner that represents the number of minutes to wait between consecutive scans.

SharePoint Discovery Task Wizard - Policies

Field	Description
All discovery policies	Select this radio button if you want all discovery policies to be applied in this scan. Websense Data Security will search for data that matches the rules in all deployed policies.
Selected policies	Select this radio button if you want only certain policies to be applied in this scan, then select the policies to apply.

SharePoint Discovery Task Wizard - File Filtering

Field	Description
Filter by Type	Select this check box if you want to filter the files to scan by file type, then indicate what file types to include in the scan and what exceptions to make, if any.
Include file types	List the types of files to be scanned, separated by semi-colons. You can use the "*" or "?" wildcards. For example, "*.doc; *.xls; *.ppt; *.pdf" Click **File Types** to select the file types to include by extension. You can add or edit file types in the resulting box if necessary. To set Data Security to scan all files, set **Include file types** to *.
Except	List the file types to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.
Filter by Age	Select this check box if you want to filter the files to scan by file age. Then select one of the following radio buttons:
Scan only files that were modified:	◆ **Within** - Select this button if you want to search only for files that were modified within a certain period, then indicate the period (in months) using the spinner. ◆ **More than** - Select this button if you want to search only for files that were modified more than a certain number of months ago, then specify the number using the spinner. ◆ **Between** - Select this button if you want to search for files modified between 2 dates, and specify the dates.
Filter by Size	Select these options if you want to filter the files to scan by file size. You can select one or both of the check boxes.
Scan only files larger than	Select this box to scan only files *larger* than a certain size, then use the spinner to specify the size.
Scan only files smaller than	Select this box to scan only files *smaller* than a certain size, then use the spinner to specify the size.

Note

Only the latest version of a document is scanned, not the entire document history. In addition, only files are scanned, not other information containers such as tasks.

SharePoint Discovery Task Wizard - Advanced

Field	Description
No limit	Select this radio button if you do not want to limit the bandwidth used for the discovery process.
An average of (1-9999) Mbps	Select this radio button if want to limit the bandwidth used for the discovery process to an average number of megabytes per second, then select the desired limit. This prevents strain on your SharePoint servers, network adapters, and on the Websense Data Security system.
Full scan schedule	Select one of the following radio buttons to indicate when you want to perform full discovery scans: ◆ **Only on policy update** - Select this option if you want to perform full discovery only when a discovery policy changes. ◆ **On policy update or fingerprinting classifier update** - Select this option if you want to perform full discovery when a discovery policy *or* a fingerprinting version changes. ◆ **Always** - Select this option if you want to perform full discovery on the scheduled time no matter what has changed. (We don’t recommend choosing “always,” because this slows the discovery process and taxes the system and file servers.)

SharePoint Discovery Task Wizard - Finish

Displays a summary of the SharePoint discovery task you just established.

Database tasks

The wizard for creating database discovery tasks has 7 pages:

- *Database Discovery Task Wizard - General*
- *Database Discovery Task Wizard - Data Source Name*
- *Database Discovery Task Wizard - Scheduler*
- *Database Discovery Task Wizard - Policies*
- *Database Discovery Task Wizard - Table Filtering*
- *Database Discovery Task Wizard - AdvancedDatabase Discovery Task Wizard - Advanced*
- *Database Task Wizard - Finish*

Database Discovery Task Wizard - General

Field	Description
Name	Enter a name for this discovery task.
Description	Enter a description for this discovery task.
Crawler	Select the crawler to perform the scan. Typically, this is the crawler that is located in closest proximity to the database server.

Database Discovery Task Wizard - Data Source Name

Field	Description
Data source name	Select a data source name (DSN) from the drop down list. If you've not created a DSN for the database yet, refer to *Preparing for fingerprinting*, page 90 for information.
Use the data source credentials	Select this option if you want to use the credentials set up for the data source. Not all DSNs have the option to store credentials.
Use the following credentials	Select this option if you want to use specific credentials, then specify the credentials.
User name	Enter the user name of any user with "read" privileges to the database.
Password	Enter and confirm a password for this user.
Domain	Optionally, enter the domain for the entered user.

Database Discovery Task Wizard - Scheduler

Field	Description
Enabled	Select this check box to enable the scheduler for the current task. Deselect **Enabled** to gain manual control over the task. When the scheduler is disabled, you can start and stop tasks using the scan controls on the toolbar.
Run scan	Select how often you want to run the scan process: once, daily, weekly, or continuously.
Hours to perform the scan	If you choose **Daily** or **Weekly**, specify the hours in which you want to run the scan, for example, daily at 2 a.m.
But not before	If you select **Once** or **Continuously**, this check box appears. Select it if you want to run the scan as soon as possible, but not before a designated time or date. Then select a date from the pull-down box and a time from the spinner.
Wait xx minutes between consecutive scans	If you select **Continuously**, this option appears. Select a number from the spinner that represents the number of minutes to wait between consecutive scans.

Database Discovery Task Wizard - Policies

Field	Description
All discovery policies	Select this radio button if you want all discovery policies to be applied in this scan. Websense Data Security will search for data that matches the rules in all deployed policies.
Selected policies	Select this radio button if you want only certain policies to be applied in this scan, then select the policies to apply.

Database Discovery Task Wizard - Table Filtering

Field	Description
Include tables	Enter the user names, schemas, or table names to scan, separated by semicolons.
Except	Enter the user names, schemas, or table names not to scan.

✓ **Note**

The discovery filtering mechanism uses a specific full path search pattern. In order for tables to be detected within the full path, follow the structure described below. The Discovery search pattern is matched as follows: [Catalog.Schema.Table] Use an asterisk (*) before the Database entry type, i.e. *.TB_123, only if the ending of the full path ends with .TB_123. For instance: MyDB.Sys.**TB_123**. Use and asterisk (*) before and after the Database entry type, i.e. *.Sys.*, for entries that may have entries before and after it in the full path. For instance: MyDB**.Sys.**TB_123.

Database Discovery analyzes the data in 5000-record chunks. Each chunk is treated independently and all policy thresholds are validated against a single chunk. No aggregation of analysis results is accumulated over the entire table. Therefore, if a policy keyword has a threshold of 10 and this keyword is detected 3 times in each of 5 chunks, no breach is triggered.

Database Discovery Task Wizard - Advanced

Field	Description
No limit	Select this radio button if you do not want to limit the bandwidth used for the discovery process.
An average of (1-9999) Mbps	Select this radio button if want to limit the bandwidth used for the discovery process to an average number of megabytes per second, then select the desired limit. This prevents strain on your database servers, network adapters, and on the Websense Data Security system.
Discovery sample	Select one of the following radio buttons to indicate whether you want Data Security to scan all records of each table, or just a segment. ◆ **Segment scan to** - Select this option to scan X records from the table (the X records are chosen randomly); this will not scan the entire table. ◆ **Scan all records of each table** - Select this option if you want to to scan all records. This can affect performance.

Database Task Wizard - Finish

Displays a summary of the database discovery task you just established.

Exchange tasks

The wizard for creating Exchange discovery tasks has 8 pages:

- *Exchange Discovery Task Wizard - General*
- *Exchange Discovery Task Wizard - Exchange Servers*
- *Exchange Discovery Task Wizard - Mailboxes & Folders*
- *Exchange Discovery Task Wizard - Scheduler*
- *Exchange Discovery Task Wizard - Policies*
- *Exchange Discovery Task Wizard - File Filtering*
- *Exchange Discovery Task Wizard - Advanced*
- *Exchange Discovery Task Wizard - Finish*

Exchange Discovery Task Wizard - General

Field	Description
Name	Enter a name for this discovery task.
Description	Enter a description for this discovery task.
Crawler	Select the crawler to perform the scan. Typically, this is the crawler that is located in closest proximity to the Exchange server.

Exchange Discovery Task Wizard - Exchange Servers

Field	Description
Click here	Click this link to view the Exchange servers that will be scanned. These are the servers that have already been resolved.
User name	Enter the user name of an administrator with access to the Exchange servers.
Password	Enter and confirm a password for this administrator.
Domain	Optionally, enter the domain for the entered administrator user.
Connect using secure HTTP	Select this option if you want Data Security to connect to your Exchange server using HTTPS and SSL. **Note:** Not all Exchange servers are set up for HTTPS. By default, Exchange 2003 is configured for HTTP and Exchange 2007 is configured for HTTPS. Check the settings on your Exchange server before selecting this option.
Additional servers	Websense Data Security tries to calculate which Exchange servers host each mailbox and public folders, and on rare cases fails to find one or more of the servers. Use this setting to explicitly specify Exchange servers that should be scanned. Enter the host name or IP address of the additional server and click **Add**.

Exchange Discovery Task Wizard - Mailboxes & Folders

Field	Description
Mailboxes	By default, discovery runs on no mailboxes. Click **Edit** to select the mailboxes to scan. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool.
Public mail folders	By default, discovery runs on no public mail folders. Click **Edit** to select the public mail folders to scan. An exchange discovery task can scan mailboxes, public folders, or both. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool.

✓ **Note**

The crawler scans email messages, notes, calendar items, and contacts found in the mailboxes and folders you define here.

Exchange Discovery Task Wizard - Scheduler

Field	Description
Enabled	Select this check box to enable the scheduler for the current task. Deselect **Enabled** to gain manual control over the task. When the scheduler is disabled, you can start and stop tasks using the scan controls on the toolbar.
Run scan	Select how often you want to run the scan process: once, daily, weekly, or continuously.
Hours to perform the scan	If you choose **Daily** or **Weekly**, specify the hours in which you want to run the scan, for example, daily at 2 a.m.
But not before	If you select **Once** or **Continuously**, this check box appears. Select it if you want to run the scan as soon as possible, but not before a designated time or date. Then select a date from the pull-down box and a time from the spinner.
Wait xx minutes between consecutive scans	If you select **Continuously**, this option appears. Select a number from the spinner that represents the number of minutes to wait between consecutive scans.

Exchange Discovery Task Wizard - Policies

Field	Description
All data discovery policies	Select this radio button if you want all discovery policies to be applied in this scan. Websense Data Security will search for data that matches the rules in all deployed policies.
Selected policies	Select this radio button if you want only certain policies to be applied in this scan, then select the policies to apply.

Exchange Discovery Task Wizard - File Filtering

Field	Description
Filter by Mailbox or Folder name	Select this check box if you want to filter the scan by mailbox or folder name, then indicate what names to include and exclude, if any. Wildcards are allowed.
Filter by Subject	Select this check box if you want to filter the scan by item subject lines (among them email, calendar items, notes, contacts, etc.), then indicate what subjects to include and exclude, if any.
Filter by Age	Select this check box if you want to filter the scan by age. Then select one of the following radio buttons: ◆ **Within** - Select this button if you want to search only for items that were modified within a certain period, then indicate the period (in months) using the spinner. ◆ **More than** - Select this button if you want to search only for items that were modified more than a certain number of months ago, then specify the number using the spinner. ◆ **From** - Select this button if you want to search for items that were modified between 2 dates.
Filter by Size	Select this check box if you want to filter the scan by size. You can select one or both of the following check boxes: ◆ **Only items larger than** - Select this box to scan only items *larger* than a certain size, then use the spinner to specify the size. ◆ **Only items smaller than** - Select this box to scan only items *smaller* than a certain size, then use the spinner to specify the size.

Exchange Discovery Task Wizard - Advanced

Field	Description
No limit	Select this radio button if you do not want to limit the bandwidth used for the discovery process.
An average of (1-9999) Mbps	Select this radio button if want to limit the bandwidth used for the discovery process to an average number of megabytes per second, then select the desired limit. This prevents strain on your Exchange servers, network adapters, and on the Websense Data Security system.
Full Scan	Select one of the following radio buttons to indicate when you want to perform full discovery scans: ◆ **Only on Data Discovery Policy update** - Select this option if you want to perform full discovery only when a discovery policy changes. ◆ **On Discovery policy update or fingerprinting version updates** - Select this option if you want to perform full discovery when a discovery policy *or* a fingerprinting version changes. ◆ **Always** - Select this option if you want to perform full discovery on the scheduled time no matter what has changed. (We don't recommend choosing "always," because this slows the discovery process and taxes the system and file servers.)

Exchange Discovery Task Wizard - Finish

Displays a summary of the endpoint discovery task you just established.

Scheduling endpoint discovery tasks

Select **Policy Management > Data Discovery Tasks > Endpoint Tasks** to configure discovery on your endpoint machines. The resulting screen displays all of the endpoint discovery tasks that have been established to date.

To create a new endpoint task, click **New**. A wizard appears.The wizard for creating endpoint discovery tasks has 7 pages:

- *Endpoint Discovery Task Wizard - General*
- *Endpoint Discovery Task Wizard - Endpoints*
- *Endpoint Discovery Task Wizard - Scheduler*
- *Endpoint Discovery Task Wizard - Policies*
- *Endpoint Discovery Task Wizard - File Filtering*
- *Endpoint Discovery Task Wizard - Advanced*
- *Endpoint Discovery Task Wizard - Finish*

Endpoint Discovery Task Wizard - General

Field	Description
Name	Enter a name for this discovery task.
Enabled	Select this check box to enable the endpoint discovery task.
Description	Enter a description for this discovery task.

Endpoint Discovery Task Wizard - Endpoints

Field	Description
Edit	By default, discovery will run on all endpoint machines. Click **Edit** to select the endpoint to scan. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool.

Endpoint Discovery Task Wizard - Scheduler

Field	Description
Run scan	Select how often you want to run the scan process: daily or weekly.
Hours to perform the scan	Specify the hours in which you want to run the scan, for example, daily at 2 a.m.
Scan only while computer is idle	Select this check box if you want to perform the discovery scan only on idle computers. This is desirable, because endpoint scanning consumes resources and can slow performance.
Pause scanning while computer is running on batteries	Select this check box if you want to pause discovery scanning if the endpoint computer switches to battery mode.

Endpoint Discovery Task Wizard - Policies

Field	Description
All data discovery policies	Select this radio button if you want all discovery policies to be applied in this scan. Websense Data Security will search for data that matches the rules in all deployed policies.
Selected policies	Select this radio button if you want only certain policies to be applied in this scan, then select the policies to apply.

Endpoint Discovery Task Wizard - File Filtering

Field	Description
Filter by Type	Select this check box if you want to filter the files to scan by file type, then indicate what file types to include in the scan and what exceptions to make, if any.
Include file types	List the types of files to be scanned, separated by semi-colons. You can use the “*” or “?” wildcards. For example, “*.doc; *.xls; *.ppt; *.pdf” Click **File Types** to select the file types to include by extension. You can add or edit file types in the resulting box if necessary. To set Data Security to scan all files, set **Include file types** to *.
Except	List the file types to exclude from the scan, separated by semi-colons. Wildcards are permitted here as well.
Filter by Age	Select this check box if you want to filter the files to scan by file age. Then select one of the following radio buttons:
Scan only files that were modified:	◆ **Within** - Select this button if you want to search only for files that were modified within a certain period, then indicate the period (in months) using the spinner. ◆ **More than** - Select this button if you want to search only for files that were modified more than a certain number of months ago, then specify the number using the spinner. ◆ **Between** - Select this button if you want to search for files modified between 2 dates, and specify the dates.
Filter by Size	Select this check box if you want to filter the files to scan by file size. You can select one or both of the check boxes.
Scan only files larger than	Select this box to scan only files *larger* than a certain size, then use the spinner to specify the size.
Scan only files smaller than	Select this box to scan only files *smaller* than a certain size, then use the spinner to specify the size.

Endpoint Discovery Task Wizard - Advanced

Field	Description
Full Scan Schedule	Select one of the following radio buttons to indicate when you want to perform full discovery scans: ◆ **Only on policy update** - Select this option if you want to perform discovery only when a discovery policy changes. ◆ **On policy update or fingerprinting classifier update** - Select this option if you want to perform discovery when a discovery policy *or* a fingerprinting version changes. ◆ **Always** - Select this option if you want to perform discovery on the scheduled time no matter what has changed.
Manage File Access Time	Select **Preserve original access time** if do not want Websense Data Security to alter the timestamp on files it scans. By default, it updates the “Last Accessed” timestamp of each file it scans. **Note:** To preserve access time, you must give Data Security read-write privileges for all hosts where discovery is being performed.

Endpoint Discovery Task Wizard - Finish

Displays a summary of the endpoint discovery task you just established.

9 Viewing Incidents and Reports

Related topics:

- *The report catalog*, page 161
- *Viewing the incident list*, page 175
- *Viewing the dashboard*, page 192
- *Viewing top violated policies*, page 194
- *Viewing incidents by severity and action*, page 194
- *Viewing top sources and destinations*, page 194
- *Viewing incident trends*, page 194
- *Viewing assessment reports*, page 195
- *Viewing sensitive data reports*, page 195

To view incidents and reports on incidents, select **Main** > **Incidents & Reports** > **Data Usage** or **Data Discovery**. Here you can view an incident list and details for individual incidents or you can choose from a catalog of reports. Several built-in reports are provided. The ones you've viewed most recently are displayed on the main Incidents & Reports page in a section called Recent Reports. The order of these reports changes with use.

Listed below are the most common reports.

✓ **Note**

What you can see depends on your permissions. See *Setting preferences for incidents and reports*, page 210 for instructions on configuring settings for incidents and reports.

Report	Description
Report Catalog	See a list of all the reports that are available, both built-in and user-defined.
Data usage reports	

Report	Description
Incidents - last 3 days (last 30 days)	View a list of all the incidents for the last 3 or 30 days. See detailed information on each incident. Investigate the violated policies and the actions taken by Websense software. Evaluate whether policy changes are needed. Select this report when you want to manage incident workflow, remediation, and escalation.
Dashboard - last 7 days	This report provides an overview of information leaks in the system, what actions are being taken on them, which channels are problematic and what kind of violations are being made.
Top Violated Policies - last 7 days	Find out which policies were violated most frequently over the last 7 days. Assess the security risk to your organization.
All Violations by Severity & Action - last 7 days	See incidents by the actions (permit, block, notify) and severities applied to them. Compare the ways Websense software enforces policies, and gain insight into potential policy changes.
Top Sources & Destinations - last 7 days	Find out who are the top violators involved in data leakage and the top domains where sensitive data was posted. This report contain information from the last 7 days.
Incident Trends - this quarter	View incident statistics for this quarter. Find out if the number of violations in your organization reduces over time.
Incident Status - last 7 days)	View the status of all incidents from the last 7 days.
Data discovery reports	
Incidents	View a list of recent incidents, with detailed information on each incident. Evaluate whether policy changes are needed. Select this report when you want to manage incident workflow, remediation, and escalation.
Sensitive data on file servers and SharePoint servers	Find out what vulnerable data was most violated and where it is stored. Assess the security risk to your organization.
Sensitive data in private mailboxes	Find out which policies were violated most, and in which mailboxes the violations occurred. Assess the security risk to your organization.
Sensitive data in databases	Find out which policies were violated most, and in which databases the violations are located. Assess the security risk to your organization.
Mailboxes with sensitive data	View which mailboxes contain sensitive data, and assess any violated policies in each mailbox.
Hosts with sensitive data	Find out which hosts contain sensitive information, and assess any violated policies on each host.
Databases with sensitive data	Find out which databases contain sensitive information, and assess any violated policies on each database.
Dashboard	Provides an at-a-glance view of system metrics for information leaks in the system and the actions being taken on them.

Summary reports are graphical and contain colorful executive charts. To view one of the most common reports, click its name on the relevant Incidents & Reports main page.

To see one of the other built-in reports, open the Data Usage Report Catalog or Data Discovery Report Catalog, select a report from the list, and select **Run** from the report's toolbar.

You can create your own report any time. Just open an existing report, for example Incidents - last 3 days, click **Manage Report > Edit Filter** to change the filters, then click **Manage Report > Save As**. Custom reports appear in the report catalog along with the built-in reports.

The report catalog

Related topics:

- *Scheduling tasks*, page 173
- *Scheduling a new task*, page 173
- *Running a scheduled task now*, page 174

To see a catalog of all the incident reports that are available:

1. Select **Main > Incidents & Reports > Data Usage** or **Data Discovery.**
2. Select **Data Usage Report Catalog** or **Data Discovery Report Catalog**.

The resulting screen lists all of the reports that are available—both built-in and user-defined.

Click a folder to expand it and see a list of related reports. Reports with this icon (▤) are detail reports of incident lists. Reports with this icon (◕) are graphical summaries.

Click the **Expand All** or **Collapse All** buttons to expand or collapse all folders, or click **New Folder** to create a new folder. You can then drag and drop reports into the new folder. You can also click the **Edit** button to edit a folder name or **Delete** to delete a folder.

Click a report to read a description about it. When you select a report, a menu bar appears. Using the report's menu bar, you can run, edit, or copy the report, export it to PDF or CSV file, schedule it to be delivered, or delete it.

Button	Icon	Description
Run	▶	Run the selected report and display it.
Edit	✎	Edit or apply filters to the report.
Copy	⧉	Copy the report.
Export to PDF	PDF	Export the report to a PDF file.
Export to CSV	CSV	Export the report to a CSV file.
Schedule a task	16	Schedule this report for automatic email delivery.
Delete	✗	Delete the selected report.

There are additional buttons in the report catalog toolbar:

Button	Icon	Description
Scheduled Tasks	16	Lets you create a schedule when incident reports should be emailed. You create a scheduled task, define sender and recipient names, and define the outgoing mail gateway.
Settings	🔧	Lets you set preferences for incident lists and reports. For example, for data usage incidents, you can define attachment size and forensics settings. For data discovery incidents, you can set database thresholds. You can also define general settings, like filtering and printing, that apply to all types of incidents. For information on configuring these settings, see *Setting preferences for incidents and reports*, page 210.

Editing a report

Editing a summary report (◕) from the report catalog opens 2 tabs:

- *General tab*
- *Filter tab*

Editing a details report (▤) opens a third tab:

- *Table Properties tab*

Complete the fields as follows.

(For information on editing a trend report, see *Editing a trend report*.)

General tab

Field	Description
Name	The name of the current report.
Description	A description of the current report.
Availability	Select who should have access to the current report: ◆ **Report owner** - Select this option if you want only the report owner to have access to this report. ◆ **All administrators** - Select this option if you want all Data Security administrators to have access to this report.
Show top	This options applies to details reports only. Select the number of items to display in the Top Items charts for this report. You can display between 1 and 20 items. For example, you can display the top 5 policies in the Top Policies chart.

Filter tab

The Filter tab enables you to narrow down the data that is displayed in the report to that which is the most relevant to you. For example, you can apply the Action filter and display only incidents with the action Block. You can apply as many filters as you require.

1. Select the filter(s) to apply to this report by checking the boxes next to the filter name.
2. Apply properties to a filter by clicking a filter name and making selections in the Filter Properties pane.

The filters that are available vary depending on whether this is a *Data Usage report* or *Data Discovery report*. Filters and their properties are described below.

Data Usage report

Filter	Description
Action	The **Action** filter enables you to filter incidents by the action (including those on endpoints) that was performed on the incident. Select the check box for each action to be displayed.
Application Name	The **Application Name** filter enables you to filter incidents by the name of applications found in the incidents. In the field, enter the list of applications to be displayed, separated by commas.
Assigned to	The **Assigned to** filter enables you to filter incidents by the person to whom they are assigned. **Unassigned** displays all incidents that have not been assigned to any administrator. Because filters can be available for all administrators, checking the **Assigned to current administrator** check box displays incidents assigned to the administrator who is currently logged onto TRITON - Data Security. **Assigned to selected administrators** enables you to select specific administrators whose assigned incidents you want to display.
Business Unit	The **Business Unit** filter enables you to filter incidents by the business unit to which they’re assigned.
Channel	The **Channel** filter enables you to limit which channels’ events are displayed. Select each channel to be displayed. The list of available channels depends on channels configured in TRITON - Data Security.
Content Classifier Name	The **Content Classifier Name** filter enables you to select which specific content classifiers should be displayed in the incident list.
Content Classifier Type	The **Content Classifier Type** filter enables you to select which content classifier type should be displayed in the incident list (key phrases, dictionaries, etc.)
Destination	The **Destination** filter sets the incident list to display only incidents intercepted that were directed at specific destinations. You can select destinations from your resource list or enter them as free text. Choose which method you want to use from the pull-down list. See *Selecting items to include or exclude in a policy*, page 47 for more details on using this selector.
Detected by	The **Detected by** filter sets the incident list to display only incidents intercepted that were detected by specific Websense Data Security modules. Select each module to be displayed. The list of available modules depends on which modules configured on the TRITON - Data Security System Modules page.
Endpoint Type	The **Endpoint Type** filter enables you to filter incidents according to the type of endpoint client, e.g. laptop or desktop. In the **Filter Properties** pane, select the endpoint type.

Filter	Description
Event Time	This filter allows you to select a time for the events you want to display. For filter properties, select one of the following: ◆ **Last xx days** - Select this radio button if you want to display events from the last xx days, then select the number of days from the spinner. ◆ **Date range** - Select this radio button if you want to display events that transpired in a particular date range, then select the range from the drop-down list. Example: last 24 hours or this week. ◆ **Exact dates** - Select this radio button if you want to display events that transpired during a specific period, then select the **From** and **To** dates from the drop-down lists.
File Name	This filter enables you to filter in or out incidents according to their attachments. Click the **Display only incidents with attachments or files** radio button to view only incidents with attachments. These attachments can be filtered based on size or file name by checking the **Limit files as follows** check box. To set the filter to display incidents with with attachments of a certain size, click the radio button and set a size (in KB). To set the filter to display incidents with specific files, enter the file name (wildcards can be used), and click **Add**.
Ignored Incident	The **Ignored Incident** filter lets you filter in or out ignored incidents. By default, ignored incidents are filtered out of all reports.
Incident Tag	**Incident Tags** let you filter incidents by a tag you earlier defined. (See *Tagging incidents*, page 183). Select the tags by which to filter the report. You can use these tags to group incidents for external applications.
Incident Time	This filter lets you filter incidents by time. Use it to select the time for the events you want to display.
Maximum Matches	The **Maximum Matches** filter allows you to filter according to the rule that triggers the most matches. For example, if rules A, B, and C trigger incidents in MyPolicy; the one that has the most matches would be included.
Policy	Use the check boxes provided to set which policy's incidents are displayed in the incident list.
Severity	Use this filter to select the severity of incidents to display. Select **High** if you want to display incidents of high severity, and so on. Select as many severity levels as desired.
Source	The **Sources to include** filter sets the incident list to display only incidents intercepted that were directed at specific sources. You can select destinations from your resource list or enter them as free text. Choose which method you want to use from the pull-down list. See *Selecting items to include or exclude in a policy*, page 47 for more details on using this selector.
Status	The **Status** filter enables you to select which incidents per status to be displayed in the incident list.
Total Size	This filter enables you to select the size of incidents to display. You can display incidents greater than a certain size (in kilobytes), or between 2 sizes.
Violation Triggers	The **Violation Triggers** filter enables you to select which Violation Triggers' incidents are displayed in the incident list. In the field, enter the list of violation triggers to be displayed, separated by commas.

Data Discovery report

Filter	Description
Assigned to	The **Assigned to** filter enables you to filter incidents by the person to whom they are assigned. **Unassigned** displays all incidents that have not been assigned to any administrator. Because filters can be available for all administrators, checking the **Assigned to current administrator** check box displays incidents assigned to the administrator who is currently logged onto TRITON - Data Security. **Assigned to selected administrators** enables you to select specific administrators whose assigned incidents you want to display.
Channel	The **Channel** filter enables you to limit which channels' events are displayed. Select each channel to be displayed. The list of available channels depends on channels configured in TRITON - Data Security.
Content Classifier Name	The **Content Classifier Name** filter enables you to select which specific content classifiers should be displayed in the incident list.
Content Classifier Type	The **Content Classifier Type** filter enables you to select which content classifier type should be displayed in the incident list (key phrases, dictionaries, etc.)
Date Accessed	If you want to see when data in violation of policy was accessed, use this filter, then select the dates and times you want to see. Events relating to the access dates you choose are shown in the report. You can display events for data that was accessed within the last x days, within a date range, or on exact dates. You can also specify time periods.
Date Created	If you want to see when a file in violation of policy was created, use this filter, then select the dates and times you want to see. Events relating to the creation dates you choose are shown in the report. You can display events for data that was created within the last x days, within a date range, or on exact dates. You can also specify time periods.
Date Modified	If you want to see when a file in violation of policy was modified, use this filter, then select the dates and times you want to see. Events relating to the modify dates you choose are shown in the report. You can display events that transpired within the last x days, within a date range, or on exact dates. You can also specify time periods.
Detected by	The **Detected by** filter sets the incident list to display only incidents that were detected by specific Websense Data Security modules. Select each module of interest. The list of available modules depends on which modules configured on the TRITON - Data Security System Modules page.
Discovery Task	Use this filter to select the discovery tasks to display in the report.
Discovery Type	Use this filter to select the type of discovery to display in the report: File System, Endpoint, SharePoint, Database, and/or Exchange.
Endpoint Type	The **Endpoint Type** filter enables you to filter incidents according to the type of endpoint client, e.g. laptop or desktop. Choose the endpoint(s) to display in the right pane.

Filter	Description
Event Time	This filter allows you to select a time for the events you want to display. For filter properties, select one of the following: ◆ **Last xx days** - Select this radio button if you want to display events from the last xx days, then select the number of days from the spinner. ◆ **Date range** - Select this radio button if you want to display events that transpired in a particular date range, then select the range from the drop-down list. Example: last 24 hours or this week. ◆ **Exact dates** - Select this radio button if you want to display events that transpired during a specific period, then select the **From** and **To** dates from the drop-down lists.
Folder	This filter allows you to view incidents from a certain folder or folders. Type a valid folder name into the field box, then click **Add**.
File Name	This filter enables you to filter in or out incidents according to their attachments. Click the **Display only incidents with attachments or files** radio button to view only incidents with attachments. These attachments can be filtered based on size or file name by checking the **Limit files as follows** check box. To set the filter to display incidents with with attachments of a certain size, click the radio button and set a size (in KB). To set the filter to display incidents with specific files, enter the file name (wildcards can be used), and click **Add**.
File Owner	Use this filter to filter incidents by file owner. Type a valid owner name into the field box, then click **Add**.
Folder Owner	Use this filter to filter incidents by folder owner. Type a valid owner name into the field box, then click **Add**.
File Permissions	Use this filter to filter incidents by file permissions. Type a valid permission into the field box, then click **Add**. The values depend on the permissions of the file system the crawler scans.
File Size	Use this filter to filter incidents by file size, then choose the size of the file to include in the report.
Host Name	Use **Host Name** to filter incidents by the host on which they were detected. Type a valid host name into the field box, then click **Add**.
Ignored Incident	The **Ignored Incident** filter lets you filter in or out ignored incidents. By default, ignored incidents are filtered out of all reports.
Incident Tag	**Incident Tags** enable setting a free text tag that can link incidents gathered in TRITON - Data Security to external applications that gives tags (free text) to each incident. It also enables filtering per these tags.
Incident Time	This filter lets you filter incidents by time. Use it to select the time for the events you want to display.
IP Address	Use **IP Address** to filter incidents by the host on which they were detected. Type a valid IP address into the field box, then click **Add**.
Locked	Use this filter to include or exclude files that are locked for update.
Mailbox Type	This filter applies only to Exchange discovery. Select **Private mailbox** if you want to display incidents from private mailboxes. Select **Public mailbox** if you want to display incidents from public mailboxes. You can select both if desired.

Filter	Description
Max Matches	The **Maximum Matches** filter allows you to filter according to the rule that triggers the most matches. For example, if rules A, B, and C trigger incidents in MyPolicy; the one that has the most matches would be included.
Policy	Use the check boxes provided to set which policy's incidents are displayed in the incident list.
Severity	Use this filter to select the severity of incidents to display. Select **High** if you want to display incidents of high severity, and so on. Select as many severity levels as desired.
Status	The **Status** filter enables you to select which incidents per status to be displayed in the incident list.
Total Size	This filter enables you to select the size of incidents to display. You can display incidents greater than a certain number of KB, or between x KB and y KB.
Violation Triggers	The **Violation Triggers** filter enables you to select which Violation Triggers' Incidents are displayed in the incident list. In the field, enter the list of violation triggers to be displayed, separated by commas.

Table Properties tab

1. Select the columns to display in the table for this report. The options vary depending on whether this is a *Data Usage report* or a *Data Discovery report*.
2. Use the arrows to indicate the order of the columns.
3. Adjust the width as desired.
4. Specify the maximum number of incidents to display on any one page.
5. Select **Sort by** if you want to sort the view data by one of the columns you selected, then choose the column from the drop-down list.
6. Indicate if you want to sort by ascending or descending values.

Data Usage report

Column	Description
Action	The action taken on the incident, as determined by the action plan. Actions include: - **Release Content** - Release quarantined content to recipients - **Assigned Incident** - Changed incident assignment from Unassigned - to administrator. Changed incident assignment from administrator to Unassigned - **Ignored Incidents** - Marked incident as ignored - **Ignored Incidents unmark** - Ignored status is removed from incident - **Change Status** - Changed incident status from New to In Process or from In Process to Closed. - **Change Sensitivity** - Changed incident sensitivity. - **Execute Command** - Executed remediation script.
Analyzed by	Displays the name of the server component that analyzed the incident.
Assigned to	Either Unassigned or the name of the administrator assigned to handle this incident. (See *Assigning incidents*, page 180.)
Channel	The channel where the incident occurred. Possible channels include: - Email - Web - FTP - Endpoint application - Endpoint printing - Network printing.
Destination	The intended destination of the content that violated policy.
Details	The details listed in the forensics Properties tab. Shows the subject in an SMTP incident, the URL in a Web incident, etc.
Detected by	Displays the name of the Websense Data Security device or component that detected this incident.
Endpoint type	The type of endpoint involved in the incident: PC, laptop, etc.
Event ID	The ID number assigned to the event or transaction.
Event time	The date the event occurred.
File name	The name and size of the attachment for this incident.
ID	The incident’s unique ID number.
Incident Tag	Displays any incident tag set for the incident. (See *Tagging incidents*, page 183.)
Incident Time	The time and date the incident was detected.
Max Matches	The maximum number of violations triggered by any given rule in the incident.
Policy	The policies that were violated by the content.

Column	Description
Severity	The severity of the incident: High, Medium, or Low. You define severity in the Severity & Action page of the Add rule wizard. For example: >0 matches = Low severity; >20 = Medium; >400 = High. You can also change an incidents severity (see *Changing incident severity*, page 182).
Source	The source of the incident. Could be a person, computer, or other.
Status	The status of the incident. Possible status include: ◆ New ◆ In process ◆ Closed ◆ Under investigation See *Changing incident status*, page 181.
Total size	The total size of the file or attachment involved, if any, in megabytes.
Violation Triggers	The information that created the breach.

Data Discovery report

Column	Description
Analyzed by	Displays the name of the server component that analyzed the incident.
Assigned to	Either Unassigned or the name of the administrator assigned to handle this incident. (See *Assigning incidents*, page 180.)
Channel	The channel where the incident occurred. Possible channels include: ◆ Email ◆ Web ◆ FTP ◆ Endpoint application ◆ Endpoint printing ◆ Network printing
Details	The details listed in the forensics Properties tab. Shows the subject in an SMTP incident, the URL in a Web incident, etc.
Detected by	Displays the name of the Websense Data Security device or component that detected this incident
Discovery task	The discovery task that identified the incident.
Discovery type	The type of resource that was scanned: File System, Endpoint, SharePoint, Database, and/or Exchange.
Endpoint type	The type of endpoint involved in the incident: PC, laptop, etc.
Event ID	The ID number assigned to the event or transaction.
Event time	The date the event occurred.
File extension	The file extension of the file that violated policy. For example: .docx or .pptx.
File full path	The full directory path of the file that violated policy.
File name	The name of the file that violated policy.
File owner	The owner of the file that contained the policy violation.
File size	The size of the file that violated policy.
Folder	The folder of the file that violated policy.
Host name	The name of the host on which the violation was detected.
ID	The incident’s unique ID number.
Ignored incident	The incidents marked as ignored.
Incident Tag	Displays any incident tag set for the incident. (See *Tagging incidents*, page 183.)
Incident Time	The time and date the incident was detected.
IP address	The IP address of the host on which the violation was detected.
Locked	Indicates whether the incident is locked or available for updates.
Max Matches	The maximum number of violations triggered by any given rule in the incident.

Column	Description
Policy	The policies that were violated by the content.
Severity	The severity of the incident: High, Medium, or Low. You define severity in the Severity & Action page of the Add rule wizard. For example: >0 matches = Low severity; >20 = Medium; >400 = High. You can also change an incidents severity (see *Changing incident severity*, page 182).
Status	The status of the incident. Possible status include: • New • In process • Closed • Under investigation See *Changing incident status*, page 181.
Violation Triggers	The information that created the breach.

Editing a trend report

To edit a trend report, complete the fields as follows. Note that when editing a predefined trend report, only the **Show top** field is configurable. The remaining fields apply only to custom trend reports.

Field	Description
Name	The name of the current report.
Description	A description of the current report.
Availability	Select who should have access to the current report: • **Current administrator** - Select this option if you want only the current administrator to have access to this report. • **All administrators** - Select this option if you want all Data Security administrators to be able to view, edit, and delete this report.
Show top	Select the number of items to display in the Top Items charts for this report. You can display between 1 and 20 items. For example, you can display the top 5 policies in the Top Policies chart.
Last	Select this radio button if you want to display trends for the last few days, then select the exact number of days.
Date range	Select this radio button if you want to display trends for date range such as this quarter or this year, then select the range from the pull-down list.
Exact dates	Select this radio button if you want to display trends for exact dates, then select the From and To dates of interest.

Scheduling tasks

Related topics:

- *Scheduling a new task*, page 173
- *Running a scheduled task now*, page 174

From either the data usage or data discovery report catalog, click **Scheduled Tasks** to view a list of scheduled tasks you've created or to schedule a new task.

On the task list, you can learn the status of scheduled tasks, how often they recur, the last time they were run, their owner, and a description. Click a task name to view details about the task in the lower pane.

From this screen, click **New** to create a new task, **Delete** to delete the selected task, or **Run** run the selected task now (regardless of its schedule).

Scheduling a new task

1. Select **Main** > **Incidents & Reports** > **Data Usage** / **Data Discovery.**
2. Select the **Data Usage Report Catalog** / **Data Discovery Report Catalog**.
3. Click **New** on the toolbar.
4. On the **General** tab, complete the fields as follows:

Field	Description
Task name	Enter a name for the task you are scheduling.
Enabled	Select **Enabled** to enable the task for use.
Description	Enter a description for the task.
Report type	Indicate whether you want to email a data usage or data discovery report.
Report name	Select a report from the drop-down list. This is the report that will be emailed on the schedule you define.

5. On the **Mail Settings** tab, complete the fields as follows:

Field	Description
Sender name	Enter the name of the person from whom the report should be sent. This is the name that will appear in the email **From** field.
Sender email address	Enter the email address of the person from whom the report should be sent.
Outgoing mail server	The outgoing mail server that's been configured appears on screen. If you want to change the server used, click **Edit** (the pencil icon).

Field	Description
Subject	Type the subject of the message containing the report. This appears in the email **Subject:** line.
Recipients	Define the recipient(s) for the notification. Click **Edit** to select to select users or groups from a user directory. Select **Additional email addresses** if you want to send the report to someone not on your user directory list, then enter the email address. Separate multiple addresses with commas.

6. On the **Schedule** tab, complete the fields as follows:

Field	Description
Start	Select the date and time on which to start the schedule. This is the date and time of the Data Security Server.
Recurrence	Select this check box to set up a recurrence pattern for the task, then select the pattern: ◆ **Daily** - Select daily if you want the task performed every day at the same time. ◆ **Weekly** - Select weekly if you want the task to recur every week on a certain day, then select the day of the week. ◆ **Monthly** - Select monthly if you want the task to recur every month, then enter the day or range of days on which it should occur. For example, if you want the task to be performed on the 3rd of each month enter “3”. If you want it performed on the 3rd and 15th, enter “3, 15”. And if you want it performed anytime between the 27th and 31st of each month, enter “27-31”. Select one of the following radio buttons if you specify a recurrence pattern: ◆ **No end date** - Select this option if there is no end date for the recurrence. You want it to continue until you reconfigure the task. ◆ **End by** - Select this option if you want the task to end by a certain date, then select the date from the pull-down list. ◆ **End after** - Select this option if you want the task to end after a set number of occurrences, then select the number from the spinner.

7. Click **OK** when you’re done.

Running a scheduled task now

If you have created a task that sends an incident report on a certain schedule, but you want Data Security to run the report and email it now:

1. Select **Main > Incidents & Reports > Data Usage / Data Discovery.**
2. Select the **Data Usage Report Catalog / Data Discovery Report Catalog**.
3. Click **Scheduled Tasks** on the toolbar.
4. Select the task you want to run now.

5. Click **Run**.
6. When asked to confirm this action, click **OK**.

Viewing the incident list

Related topics:

- *Previewing incidents*, page 178
- *Managing incident workflow*, page 180
- *Remediating incidents*, page 184
- *Escalating incidents*, page 185
- *Managing incident reports*, page 187
- *Tuning policies*, page 191

To view a list of data usage incidents from the last 3 days, and their details:

1. Select **Main** > **Incidents & Reports** > **Data Usage.**
2. Select **Incidents - last 3 days**.

To view a list of data discovery incidents and their details:

1. Select **Main** > **Incidents & Reports** > **Data Discovery.**
2. Select **Incidents**.

The top portion of the resulting screen lists incidents, their status, the action taken, and many more details.

The incidents list is a table displaying all data usage or data discovery incidents. By default, incidents are sorted by their event time, but you can sort them (ascending or descending) by any of the columns in the table. For each incident, a quick preview of the data is provided. You can customize the types of details shown. (See *Editing table properties*, page 187.)

Click the down arrow on column header to sort, filter, or group incidents by that column. (See *Applying a column filter*, page 188 for more information.) Or click **Table Properties** ( )to change the columns that are displayed, their order, and their width. Refer to *Table Properties tab*, page 168 for a description of each property.

Use the radio controls ' |◀ ◀ 1 ▶ ▶| to jump to the first, last, previous, or next incident in the list.

Select an incident to view details about it in the bottom portion of the screen. (See *Previewing incidents*, page 178 for more information on what is displayed.)

Use toolbar buttons to manage incident workflow, remediate incidents, escalate incidents, change incident filters or table properties, and more.

Toolbar buttons

There are several buttons on the incident toolbar:

Button	Icon	Description
Workflow	✓	Click this button to manage the workflow of the selected incident, then select one of the following: • **Assign** - Select this option to assign the incident to someone or mark it as unassigned. • **Lock** - Select this option to lock the selected incident, preventing any further changes from future scans of the file. This option applies only to discovery incidents. • **Unlock** - Select this option to unlock a locked incident, allowing information from future scans to overwrite the current data. This option applies only to discovery incidents. • **Change Status** - Select this option to change the incident status or change the status labels. • **Change Severity** - Select this option to change the incident severity assignment. • **Ignore Incident** - Select this option to mark an incident as ignored or unmark an ignored incident. Mark an incident as ignored when you've reviewed it and no action is required. • **Tag Incident** - Select this option to associate an incident with a custom tag that you can later use in filters. • **Download Incident** - Select this option to download an incident. This option applies only to data usage incidents. You can download just one incident at a time. (See *Managing incident workflow*, page 180 for details on all of these options.)
Remediate	✚	This option does not apply to Web Security Gateway Anywhere customers. Click this button to remediate the selected incident, then select one of the following: • **Release** - Select this option to release the selected incident (email message) from quarantine. This option applies only to data usage incidents on SMTP or Exchange channels. You can add a comment to the confirmation window for future reference if desired. • **Run Remediation Script** - Select this option to run a remediation script on the selected incident. (See *Remediating incidents*, page 184 for details on both options.)

Button	Icon	Description
Escalate		Click this button to escalate the selected incident to a manager or other person: • **Email to Manager** - Select this option to email the incident to a manager for action. • **Email to Other** - Select this option to email the incident to another person for action. (See *Escalating incidents*, page 185 for details on both options.)
Manage Report	N/A	Click this button to edit the filter or table properties applied to the current report, then select one of the following: • **Edit Filter** - Select this option to edit the filters applied to the report—for example, choosing a longer time period or single channel. • **Table Properties** - Select this option to customize the properties of the incident table. • **Save** - Select this option to Save the changes you made to current report. • **Save As** - Select this option to save the current report with a new name. (See *Managing incident reports*, page 187. for details on all of these options.)
Settings		Lets you set preferences for incident lists and reports. For example, for data usage incidents, you can define attachment size and forensics settings. For data discovery incidents, you can set database thresholds. You can also define general settings, like filtering and printing, that apply to all types of incidents. For information on configuring these settings, see *Setting preferences for incidents and reports*, page 210.
View		Lets you customize the view in your incident list. You can choose any of the following: • **Incident list only** - Removes the preview so that many more incidents can appear in the list. • **Incident preview only** - Removes the list so you can preview more of the incident. • **Incident list and preview** - Displays the incident list and the preview in the same window. Includes scroll bars on the incident list. • **Open preview in a new window** - Opens a preview of the incident in a new window, so you can view it in its entirety.
Print Preview		Display a preview of the current, selected, or all filtered incidents.

Button	Icon	Description
Export to PDF	🟥	Export the current, selected, or all filtered incidents to a PDF file.
Export to CSV	🟩	Export the current, selected, or all filtered incidents to a CSV file.

To preview an incident and learn more about it, click on the table row of the incident in the Incidents List. See *Previewing incidents*, page 178 for details on this portion of the window.

Previewing incidents

Details of the selected incident appear at the bottom of the screen. In this preview, you can see:

- *Violations*
- *Forensics*
- *Properties*
- *History*

To see more of the preview, select **View** > **Incident Preview Only** or **View** > **Open Preview in New Window**.

Violations

In this section, you can display violation triggers or violated rules.

- **Violated rules** displays which rules were violated by the incident. Click the information icon to view more details, such as the policy and action plan for the rule.
- **Violation triggers** displays the precise values that triggered the violation and how many of those triggers were found. Click the numeric link to view details about the trigger.

Click **Tune Policy** to update your policy for this incident. You can select any of the following:

- **Exclude Source from Rules -** Select this option to exclude the incident source from one or more of the rules.
- **Disable Policies -** Select this option to disable a policy if it is not producing the desired effect.
- **Disable Rules -** Select this option to disable a rule if it is not producing the desired effect.

See *Tuning policies*, page 191 for more information.

Forensics

The **Forensics** tab shows information about the original transaction.

For data usage incidents that occurred on an email channel, it displays the message subject, from, to, attachments, and message body. In this case, you can click links to preview or open attachments. The bottom portion of the incident screen displays the message body.

For data usage incidents that occurred on a Web channel, the forensics could include the URL category property.

For data discovery incidents, forensics includes the host name and file name.

Use the **Show as** field to select how you want the text displayed: Marked HTML, plain text, or HTML.

Marked HTML includes the HTML markup language. HTML does not.

Properties

The **Properties** tab displays incident details, such as:

- Incident number
- Severity
- Status
- Action
- Channel

It also shows information about the source and destination of the incident.

For data discovery incidents, this tab also displays:

- Detection information
- Discovery task name
- File permissions
- File details

History

The **History** tab displays the incident history, such as when it was received and when it was assigned to someone.

Click **Add Comments** to add comments to the history pane.

Managing incident workflow

Related topics:

- *Assigning incidents*, page 180
- *Changing incident status*, page 181
- *Changing incident severity*, page 182
- *Ignoring incidents*, page 183
- *Tagging incidents*, page 183
- *Downloading incidents*, page 183

Click this button to manage the workflow of the selected incident, then select one of the following:

- **Assign -** Select this option to assign the incident to someone or mark it as unassigned.
- **Change Status -** Select this option to change the incident status or change the status labels.
- **Change Severity -** Select this option to change the incident severity assignment.
- **Ignore Incident -** Select this option to mark an incident as ignored or unmark and ignored incident. Mark an incident as ignored when you've reviewed it and no action is required.
- **Tag Incident -** Select this option to associate an incident with a custom tag that you can later use in filters.

The following option is available only for data usage incidents:

- **Download Incident -** Select this option to download a data usage incident.

The following options are available only for discovery incidents:

- **Lock -** Select this option to lock an incident, preventing the addition of any information from subsequent scans.
- **Unlock -** Select this option to unlock a locked incident.
- **Delete -** Select this option to delete either the selected incident(s), or all discovery incidents.

Assigning incidents

You can assign specific administrators to an incident. In this case, other administrators, even those who can view these incidents, no longer have the ability to perform actions on this incident (with the exception of Superusers).

To assign an incident to someone for action:

1. Select the incident.
2. From the toolbar, select **Workflow** > **Assign**.

3. Select the **Assign to** radio button.
4. From the pull-down list, select the person to whom to assign the incident.
5. Add comments if desired.
6. Click **OK**.

To mark an incident as unassigned after it’s been assigned:

1. Select the incident.
2. From the toolbar, select **Workflow** > **Assign**.
3. Select the **Unassigned** radio button.
4. Add comments if desired.
5. Click **OK**.

Locking and unlocking incidents

During data discovery, a file may be scanned several times as a part of consecutive scans. Each scan may detect different policy breaches, if either the file or the policy has changed. If this happens, the incident for that file is overwritten with the most recent information.

If you want to keep the current stored information for a particular incident, you can choose to lock it. Information logged from subsequent scans on this file is then discarded.

To lock a discovery incident:

1. Select the incident.
2. From the toolbar, select **Workflow** > **Lock**.

To unlock an incident, allowing its information to be overwritten by future scans:

1. Select the incident.
2. From the toolbar, select **Workflow** > **Unlock**.

Changing incident status

There is a column for status available in the incident list. In addition, when you select an incident, its status is displayed in the incident details. To change the status of an incident:

1. Select the incident.
2. From the toolbar, select **Workflow** > **Change Status**.
3. Select a new status from the menu.

Possible statuses include:

Status Flag	Definition	Label Editable?
🚩	New	Uneditable
⚑	In Process	Uneditable
⚐	Closed	Uneditable
⚑	(User-defined)	Editable
⚑	(User-defined)	Editable

Select **Edit Labels** to customize the status labels. New, In Process and Closed are uneditable, but you can add a fourth and fifth label as needed.

Changing incident severity

The incident’s severity setting is a measure of how important it is to the organization that this incident is handled. The severity of an incident is automatically decided by Websense Data Security. This calculation takes both the prescribed severity of the incident and the number of matched violations into account.

Incident severity is displayed in the incident list. There is a column for severity. In addition, when you select an incident, its severity is displayed in the incident details. To change the severity of an incident:

1. Select the incident.
2. From the toolbar, select **Workflow** > **Change Severity**.
3. Select a new severity from the menu.

Possible severities include:

Icon	Definition
H	High. This breach is significant and may have a broad impact on the business.
M	Medium. This breach is moderate and should be reviewed.
L	Low. This breach is insignificant.

Ignoring incidents

Websense recommends you mark an incident as ignored when you've reviewed it and no action is required. This makes it easier to see what requires your attention.

You can ignore files that are determined not to be violations and incidents (files or attachments) that are not malicious. You can then filter ignored incidents in or out of a report.

By default, TRITON - Data Security does not display ignored incidents.

To mark an incident as ignored:

1. Select the incident.
2. From the toolbar, select **Workflow** > **Ignore Incident**.
3. Select **Mark as ignored incident**.

If you no longer want the incident to be ignored, you can unmark it:

1. Select the incident.
2. From the toolbar, select **Workflow** > **Ignore Incident**.
3. Select **Unmark ignored incident**.

Tagging incidents

If desired, you can add a custom tag to an incident so you can later search and filter data based on this tag. For example, you might want to tag all incidents relating to Project ABC with the string “Project ABC”. Later you can apply a filter with the string “Project ABC” to view all incidents relating to the project.

You can also tag incidents to group them together for external applications.

To tag an incident:

1. Select the incident.
2. From the toolbar, select **Workflow** > **Tag Incident**.
3. Enter the desired text string into the **Incident tag** field.
4. Add comments if desired.
5. Click **OK**.

Downloading incidents

To download incident details to your computer:

1. Select the incident.
2. From the toolbar, select **Workflow** > **Download Incident**.
3. When prompted, click **OK** to confirm the action.

Remediating incidents

Related topics:

- *Releasing incidents*, page 184
- *Running remediation scripts on incidents*, page 185

✓ **Note**

This section does not apply to Web Security Gateway Anywhere customers.

Click this button to remediate the selected incident, then select one of the following:

- **Release -** Select this option to release the selected incident from quarantine.
- **Run Remediation Script -** Select this option to run a remediation script on the selected incident.

Releasing incidents

This option is only available for blocked incidents sent from the SMTP agent, protector, or Exchange agent—that is, for email transactions that have been quarantined.

If an SMTP email transaction was quarantined, the administrator responsible for handling this incident can release this incident to the recipients originally blocked from receiving the content.

All messages are released through the configured release gateway. You configure the release gateway at **Settings** > **Configuration** > **System** > **Remediation**.

There are 2 ways to release an incident:

From the Details report

1. Select the incident or incidents you want to release.
2. From the toolbar, select **Remediate** > **Release**. A confirmation screen appears. It tells you which incidents were released successfully and which were not released due to errors, if any.
3. Add comments to the release operation if desired.
4. Click **OK**.

A confirmation window appears when the item has been released. You can add a comment to the confirmation window for future reference if desired.

By replying to the notification message

When an email incident is blocked, or indeed any policy breach is discovered, notifications are sent to all the users configured in **Main** > **Policy Management** > **Resources** > **Notifications**. Users can release email incident by replying to the notification message.

If the message was successfully released, the user who released the message receives a confirmation email.

Running remediation scripts on incidents

Related topics:

- *Remediation scripts*, page 116
- *Adding a new remediation script*, page 117

If you have added *incident management* remediation scripts under **Main** > **Policy Management** > **Resources** > **Remediation Scripts**, you can run those scripts on incidents in the incident list.

For example, if administrators want to be notified via SMS messages each time a critical incident is intercepted by Websense Data Security, an external executable file that sends SMS notifications can be applied as remediation script.

1. Select the incident or incidents on which you want to run the script.
2. From the toolbar, select **Remediate** > **Run Remediate Script**.
3. From the resulting dialog box, select the script to run. A description of the script and the script parameters are shown. You cannot edit these here.
4. If you want to change the status of the incident once the script has run, select the check box labeled **When the command is run change status to**. Select the desired status from the pull-down list.
5. Click **OK**.

Escalating incidents

Related topics:

- *Emailing incidents to your manager*, page 186
- *Email incidents to another*, page 186

Click this button to escalate the selected incident to a manager or other person.

For data usage incidents, the following options are available:

- **Email to Manager -** Select this option to email the incident to a manager for action.
- **Email to Other -** Select this option to email the incident to another person for action.

For data discovery incidents, you have the following option:

- **Email Incident -** Select this option to email the incident to the person of your choice.

Emailing incidents to your manager

1. Select the incident or incidents you want to email.
2. From the toolbar, select **Escalate** > **Email to Manager**. A screen appears.
3. By default, the message is sent to the sender's manager. If you want to send a copy or blind copy to other people, enter their email addresses in the **Cc** and **Bcc** fields.
4. Enter a subject in the **Subject** field.
5. Select **Include original message as an attachment** if you want to attach the message.
6. Select **High importance** if this is a priority message.
7. Edit the predefined message body as desired.
8. Click **OK**.

The selected incident(s) is immediately emailed to the manager.

Email incidents to another

If you want to send an incident to someone other than your predefined manager, you can do so.

1. Select the incident or incidents you want to email.
2. Do one of the following:
   - For data usage incidents, from the toolbar, select **Escalate** > **Email to Other**.
   - For data discovery incidents, from the toolbar, select **Escalate** > **Email Incident**.

   A screen appears.
3. Enter the recipient's email address in the **To** field. Enter additional email addresses in the **Cc** and **Bcc** fields.
4. Enter a subject in the **Subject** field.
5. For data usage incidents, select **Include original message as an attachment** if you want to attach the message.
6. Select **High importance** if this is a priority message.
7. Edit the message body as desired.
8. Click **OK**.

The selected incident(s) is immediately emailed to the people you selected.

Managing incident reports

Related topics:

- *Editing report filters*, page 187
- *Editing table properties*, page 187
- *Applying a column filter*, page 188
- *Saving reports*, page 189

You can change the incident report by applying different filters or editing table properties. You can then save the report with your changes or create a new report by saving it as another file.

Click the **Manage Report** link and select one of the following options:

- **Edit Filter -** Select this option to edit the filters applied to the report—for example, choosing a longer time period or single channel.
- **Table Properties -** Select this option to customize the properties of the incident table.
- **Save -** Select this option to save the changes you made to current report.
- **Save As -** Select this option to save the current report with a new name.

Editing report filters

Note

You can also apply a filter by selecting the right arrow on a column header in the incident table and selecting **Filter by [*column*]**. (See *Applying a column filter*, page 188 for more information.)

To change the filters that are applied to this report, select **Manage Report** > **Edit Filter**. See *Filter tab*, page 163 for instructions on selecting filters and defining filter properties.

Editing table properties

To edit the properties of the incident table (the one displayed at the top of the Incidents - last 3 days report), select **Manage Report** > **Table Properties**.

Using the check boxes provided, select each column to be displayed and set the maximum width in number of characters. See *Table Properties tab*, page 168 for a description of the columns.

Set the maximum number of incidents to be displayed per page (1 to 200). By default this is set to 100. This setting is saved for each administrator.

Use the up/down arrows to the right of the incident table to customize the order of columns.

Click **OK** to apply these settings.

Applying a column filter

The column filter enables you to apply filters directly to the incident list without accessing the Manage Report menu to build a custom screen.

Column filters further filter the data provided in the incident list. This means that the column filter is applied on top of the main filter—the one created with the **Manage Report > Edit Filter** option.

For example: If the main filter is set to display only SMTP channel incidents, and the column filter is then set to display severity - high, only high severity SMTP incidents are displayed. Column filters are not saved, so when a custom filter is applied, the column filter that was applied before it is lost.

Selecting the **Clear Column Filter** option clears the applied column filter and applies the selected main filter.

Arrow buttons on column headers enable users to quickly filter the displayed information. Below are instructions of how to filter the information in the columns.

To filter columns:

1. Click the down arrow button in a column header. A drop menu with 5 options appears. Different columns display different options.
2. Select from one of the following options:

Option	Description
Sort Ascending	Sorts the column’s entries by A-Z, from top to bottom.
Sort Descending	Sorts the column’s entries by Z-A, from top to bottom.
Group by this Column...	Incidents in the incident list screens can be grouped, allowing an alternative filtered report. Grouping incidents enables deep drill down into a problem. For more information, refer to Grouping Incidents (on page 212).

Option	Description
Filter by this Column...	When this option is selected, a pop-up caption box appears enabling users to filter the column according to specific words or to filter the column to exclude specific words. In the pop-up box, select one of the following options in the Must field: ◆ **Be equal to** - Enter a specific word in the text field that you want included in the column and click **OK**. ◆ **Be empty** - Enter a specific word in the text field that you want excluded in the column and click **OK**. The results are displayed in the column with or without the specific words in the column. * Note: When a column is filtered, the header arrow turns blue.
Clear Column’s Filter	When this option is selected, all current and previous filters set for the column are cleared.

Saving reports

Once you’ve applied the filters and table properties you desire, click **Manage Report > Save** or **Save As** to save your custom report. **Save** saves your changes to the current report. **Save As** lets you specify a new report name. The new report then appears in the report catalog for future use.

Grouping incidents

In the active report, you can group incidents by the person they’re assigned to, by source, by status, by channel, or a number of other headings in the incident table. Each column header has a down arrow next to it.

Select the down arrow next to the column header of interest, then select **Group by [*column*]**.

Your report is now grouped by that function.

Grouping incidents is an effective way to drill-down into a problem.

For example, grouping can be used as follows:

An administrator who wants to take a look at the most problematic channel can group by channel. This enables the administrator to quickly see that HTTP is by far the problematic channel, and can then drill-down into HTTP. Now the administrator groups by the policy category to learn that finance is the information that is most frequently leaked and within that group, the administrator can group by IP addresses to find the most problematic employee and drill down to that employee’s incidents.

See *Applying a column filter*, page 188 for additional information.

Deleting incidents

Only discovery incidents can be deleted.

To delete a single incident, locate the incident in question and select it by clicking the check box on the left. From the toolbar, select **Workflow** > **Delete** > **Delete Selected Incidents**.

To delete multiple incidents, use the display and column filters so that only the incidents you desire to delete are displayed. Select all displayed incidents. From the toolbar, select **Workflow** > **Delete** > **Delete Selected Incidents**.

To delete all discovery incidents, select **Workflow** > **Delete** > **Delete ALL Discovery Incidents**.

Printing incidents

Related topics:

- *Setting general preferences*, page 210

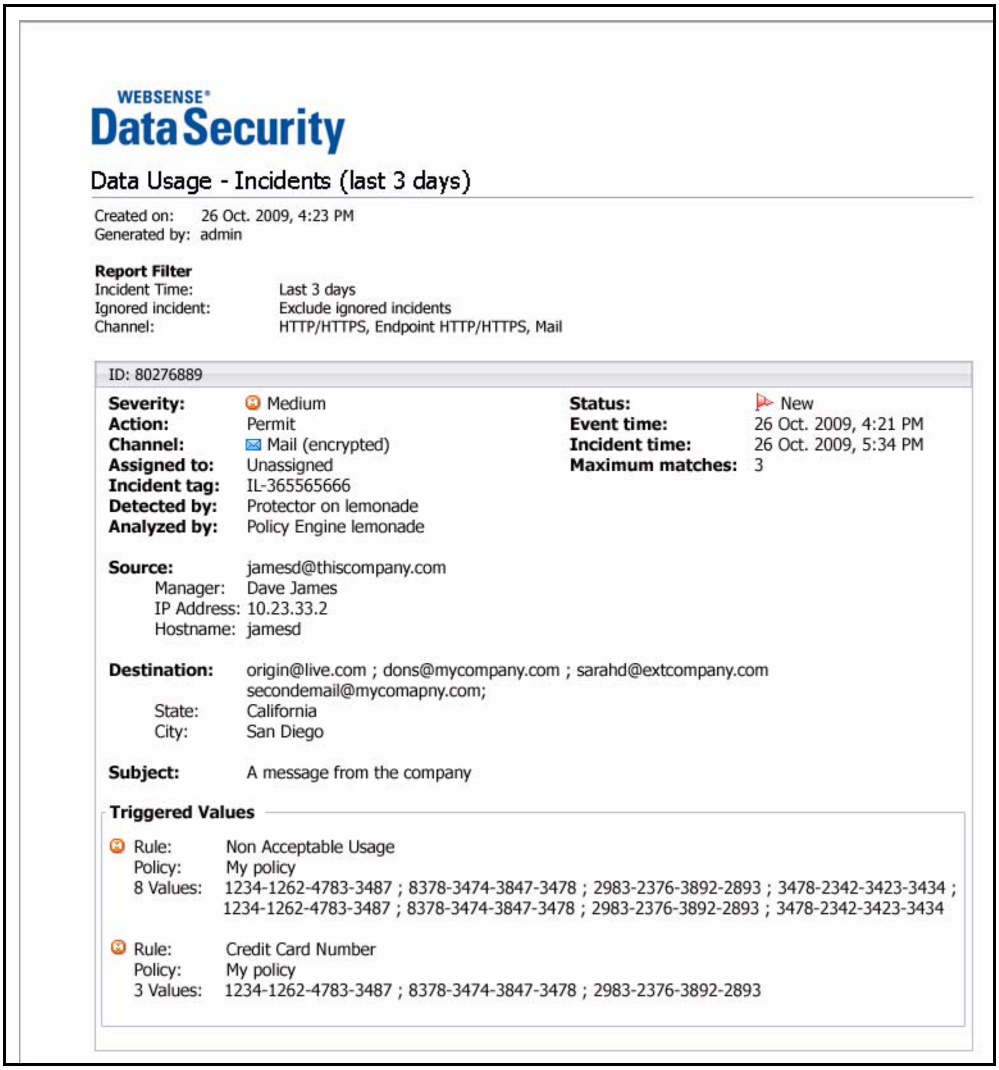
There are many ways to view or print incidents. You can:

- view a Print Preview
- export the incident to a PDF file to print it
- export the incident to a CSV file, import the CSV into your favorite program and print it.

You can print the current incident, selected incidents, or all filtered incidents.

If you choose to print all filtered incidents, your can select a range to print (for example, 200 at a time), or you can have a list of all incidents emailed to someone or to a group of people. If you want to email the list, enter the subject and recipients for the email message and click **Send**.

Here's an example of what an incident report looks like:



WEBSENSE®
Data Security

Data Usage - Incidents (last 3 days)

Created on: 26 Oct. 2009, 4:23 PM
Generated by: admin

Report Filter

Incident Time: Last 3 days
Ignored incident: Exclude ignored incidents
Channel: HTTP/HTTPS, Endpoint HTTP/HTTPS, Mail

ID: 80276889

Severity: Medium
Action: Permit
Channel: Mail (encrypted)
Assigned to: Unassigned
Incident tag: IL-365565666
Detected by: Protector on lemonade
Analyzed by: Policy Engine lemonade

Status: New
Event time: 26 Oct. 2009, 4:21 PM
Incident time: 26 Oct. 2009, 5:34 PM
Maximum matches: 3

Source: jamesd@thiscompany.com
Manager: Dave James
IP Address: 10.23.33.2
Hostname: jamesd

Destination: origin@live.com ; dons@mycompany.com ; sarahd@extcompany.com secondemail@mycomapny.com;
State: California
City: San Diego

Subject: A message from the company

Triggered Values

Rule: Non Acceptable Usage
Policy: My policy
8 Values: 1234-1262-4783-3487 ; 8378-3474-3847-3478 ; 2983-2376-3892-2893 ; 3478-2342-3423-3434 ; 1234-1262-4783-3487 ; 8378-3474-3847-3478 ; 2983-2376-3892-2893 ; 3478-2342-3423-3434

Rule: Credit Card Number
Policy: My policy
3 Values: 1234-1262-4783-3487 ; 8378-3474-3847-3478 ; 2983-2376-3892-2893

To configure how incidents are grouped when printed, see *Setting general preferences*, page 210.

Tuning policies

Often when you are first getting started, you may receive incidents that are not useful and you may realize you need to fine-tune your policies and rules. Through a process of trial and error, you can achieve a set of policies that work well for your organization.

If you want to tune a policy based on an incident:

1. Select **Main** > **Incidents & Reports** > **Data Usage** / **Data Discovery.**
2. Select **Incidents - last 3 days**.
3. Select the incident of interest. Its details are displayed in the bottom part of the screen.

4. Click the **Tune Policy** button by the incident details.
5. Select one of the following 3 options:
   - *Exclude Source from Rules*
   - *Disable Policies*
   - *Disable Rules*

Excluding source from rules

This option is for data usage incidents only.

When you select this option, a dialog box lists the rules that were breached for the selected incident. You can exclude the incident source from the rules if desired.

For example, if the source of the incident was John Doe, you can exclude John Doe from the rule in the future.

Select the rule or rules from which you want to exclude the incident source. The source is listed in the incident table in the Source column.

You can return the source to the rule later if necessary. Do this by selecting the rule in the policy management tree view, clicking **Edit**, and navigating to the **Source** tab.

Disabling policies

When you select this option, a dialog box lists the policies that were involved in the incident. If a policy is not producing the desired effect, you can temporarily disable it.

Select the policy or policies you want to disable and click **OK**.

You can enable the policies later if necessary. Do this by selecting the policy in the policy management tree view, clicking **Edit**, and selecting **Enabled**.

Disabling rules

When you select this option, a dialog box lists the rules that were breached for the selected incident. If a rule is not producing the desired effect, you can temporarily disable it.

Select the rule or rules you want to disable and click **OK**.

You can enable the rules later if necessary. Do this by selecting the rule in the policy management tree view, clicking **Edit**, and selecting **Enabled**.

Viewing the dashboard

The dashboard provides a balanced view and a high-level summary of incidents. It provides an overview of information leaks in the system, what actions are being taken on them, which channels are problematic, and what kinds of violations are being made. The report provides summaries per channel, severity, and action and provides an overall picture of information leaks on in the network.

As with all TRITON - Data Security reports, you can view the dashboard any time or create a scheduled task to receive it periodically via email.

To access the dashboard:

1. Select **Main** > **Incidents & Reports** > **Data Usage** or **Data Discovery.**
2. Select **Dashboard**.

Remember that all reports represent only incidents from to which the administrator has access.

The dashboard includes the following sections:

Data Usage Dashboard

- **Incidents by Severity -** This table displays incidents over the last 7 days by severity.
- **Incidents by Action -** This table displays incidents by the action taken on them.
- **Top 5 Channels -** This table displays incidents by channel. The corresponding pie chart displays the percentage of the total incidents represented by these channels.
- **Top 5 Policies -** This table displays incidents in the order of which policy was violated, therefore generating the most incidents.Click **Show All** to show all policies that were violated.
- **Top 5 Destination URL Categories -** This table displays URL categories with the most violations.
- **Top 5 Sources -** This table displays the sources that violated policy the most and their severity level. Click **Show All** to show all sources that violated policy.
- **Top 5 Destinations -** This table displays the destinations with the most violations and their severity level. Click **Show All** to show all destinations that were violated.
- **Top Incidents -** This table displays the top incidents as determined by severity, the maximum number of matches, and incident time. This table lists the incident ID, source, destination, severity, policy, and date/time for each incident. Click an ID number for details on the incident. Click **Show All** to show all incidents.

Data Discovery Dashboard

- **Top Policies -** This table displays the policies that were violated the most frequently and the number of times it was violated.
- **Top Items -** This table displays the hosts, mailboxes, and tables with the most violations, depending on the type of discovery performed.

You can export the dashboard report to a PDF file or view a Print Preview of it.

You can also customize the report by selecting **Manage Report** > **Edit Filter**. (See *Managing incident reports*, page 187 for more details.)

To schedule this report to be delivered by email, see *Scheduling tasks*, page 173.

Viewing top violated policies

To assess risk to your organization’s security, you should review incidents in a few key reports and consider making policy changes.

To view data usage risk:

1. Select **Main** > **Incidents & Reports** > **Data Usage.**
2. Select **Top Violated Policies - last 7 days**.

To view data discovery risk:

1. Select **Main** > **Incidents & Reports** > **Data Discovery.**
2. Select **Sensitive Data on File Servers and SharePoint Servers**.

Viewing incidents by severity and action

This table lists all incidents according to their severity and the action taken. This is useful for viewing incidents with a high severity that were blocked.

1. Select **Main** > **Incidents & Reports** > **Data Usage.**
2. Select **Severity & Action - last 7 days**.

Viewing top sources and destinations

These tables list the sources or destinations (users, addresses, email messages) that most frequently violated policies, causing the incidents listed here. These are the users whose transactions were most frequently blocked or quarantined by Websense Data Security due to breach of policy or those who were most frequently meant to receive unauthorized information.

1. Select **Main** > **Incidents & Reports** > **Data Usage.**
2. Select **Sources & Destinations - last 7 days**.

Viewing incident trends

After Websense Data Security has been running for awhile, it may be useful to see what the number of incidents was when the system was installed and if it declined over time. You can also monitor trends for specific policies over time.

1. Select **Main** > **Incidents & Reports** > **Data Usage.**
2. Select **Incident Trends - this quarter**.

The trend report displays trends for new incidents and top policies over a defined period of time, such as a quarter or year.

- **New Incidents -** Displays the number new incidents that transpired during the period, month by month.
- **Top Policies -** Lists the policies that triggered the greatest number of incidents over the time period being displayed. The graph below charts the trend of the number of incidents received over time per policy. Click **Show All** to view a list of all the policies.

To change the time period, click **Manage Report** > **Edit Filter**.

✓ **Note**

The trend report is based on aggregated data. The aggregation is done every five minutes, so incidents added in the last five minutes may not yet appear in the list.

Viewing assessment reports

The data discovery assessment reports allow you to review policy violations and see the file location, mailbox, or database in which those violations are occurring. From this you can assess the security risk to your organization and fine-tune policies accordingly.

Note that for these reports to contain information, you must first run appropriate discovery tasks. For file risk assessment, run a discovery task for endpoints, network folders, or SharePoint sites. For mailbox or database assessment, run a network discovery task for Exchange servers or databases respectively.

1. Select **Main** > **Incidents & Reports** > **Data Discovery.**
2. Select one of the following reports:
   - **Sensitive Data on File Servers and SharePoint Servers**
   - **Sensitive Data in Private Mailboxes**
   - **Sensitive Data in Databases**

Viewing sensitive data reports

The sensitive data reports enable you to see where potentially sensitive data is located in your organization, and review any violated policies for those locations.

Note that for these reports to contain information, you must first run appropriate discovery tasks. For hosts, run a discovery task for endpoints, network folders, or SharePoint sites. For mailboxes or databases, run a network discovery task for Exchange servers or databases respectively.

1. Select **Main > Incidents & Reports > Data Discovery.**
2. Select one of the following reports:
   - **Mailboxes with sensitive data**
   - **Hosts with sensitive data**
   - **Databases with sensitive data**

10 Viewing Status and Logs

TRITON - Data Security enables you to keep track of Websense Data Security traffic and events through a number of status and log screens. You can use this information to assess the performance of the system, and decide whether you need to fine-tune policy configuration.

The status and log screens are available on the Main tab, under **Status & Logs**.

Filtering data

Filtering enables you to view only the items in a list that match the criteria you specify. This narrows down the available information and makes it easier to find the data you want. For example, you can set up a filter in the audit log that displays the actions of a particular administrator on a certain date.

In most screens, you can sort, group, and filter items by column name. For example, on the endpoint status screen, you can sort endpoint hosts by IP address.

To sort or filter the table items on a status or log screen, click the down arrow by any column name and choose an option:

Field	Description
Sort Ascending	Select this option to sort the table by the active column in ascending alphabetical order.
Sort Descending	Select this option to sort the table by the active column in descending alphabetical order.
Filter by (column)	Select this option to filter the data in the table by the type of information in the active column, such as by description or task name.
Clear filter	Select this option to clear the filter and display all tasks.

To view the current filter(s) in use:

- On the endpoint status screen, click the **Filter Description** link.
- On a log screen, click the information icon ⓘ next to **Column Filtering Activated**.

Columns using a filter have a funnel icon ▽ next to the column name.

To clear a filter from a column, click the down arrow by any column name and select **Clear filter**. Additionally, many screens have a **Filter** button: clicking this button enables you to clear a single filter or all filters.

If there are too many items to fit on the screen, you can also browse the list using the Next, Previous, First, and Last buttons.

Printing and exporting logs

On many of the Status & Logs screens, you have the option to print or export to PDF or CSV file. These buttons appear in the upper right of the menu bar.

To print logs or status screens, click the **Print Preview** button.

To export them to a PDF or CSV file, click the **Export to PDF** or **Export to CSV** button.

On the endpoint status screen, you can click the down arrow next to the **Export to PDF** or **Export to CSV** button to define exactly what you want to export. You can select from the current endpoint host, the selected host, or all endpoint hosts.

Viewing the Today page

By default, the Today page opens every time you log onto TRITON - Data Security. This page shows a comprehensive view of data usage incidents that occurred in the last 24 hours, and the total number of data discovery incidents.

From the Today page, you can see any system alerts and act on them quickly and easily. You can also view incidents by host names and policy categories so you know where your greatest risks lie.

Note

The page displays only incidents that the current administrator is authorized to view.

System Alert Summary

This Today section shows relevant license information, system messages, configuration gaps, and deployment updates.

Click on an alert to see further information or take action on any issues. For example, if the System Alert Summary is displaying missing essential configurations and actions, click the link to see further details and direct links to the required fixes.

System Statistics

This section displays numerical breakdown of data collected over the last 24 hours, including:

- **Inspected Web traffic -** The number of Web transactions (including Web posts, FTP, and IM) that were analyzed
- **Inspected email messages -** The number of email messages that were analyzed.
- **Data discovery inspected items -** the number of files plus the number of database chunks scanned using network discovery. (A database chunk equals ~5000 records.)
- **Connected endpoints -** The number of endpoint clients connected to the system

Data Usage Incidents

Data Usage Incidents displays the number of data usage incidents that have been detected in the last 24 hours. Two graphs are included:

- **Incidents by Severity:** displays the number of incidents that have entered the system in the last 24 hours by severity. These include all incidents that the system has detected.

Field	Description
High	Number of incidents that have been set to the most severe setting and should be handled immediately.
Medium	Number of incidents that have been set to the medium severity setting and should be handled soon.
Low	Number of incidents that have been set to the most lenient severity setting and should be handled.

- **Top 5 Policies:** displays the policies that had the most incident violations, and the number of incidents in each of these policy categories.

The **Last data usage incident** field provides the exact date and time the last incident was logged in Websense Data Security.

Clicking the **My data usage incidents** link displays the incident summary screen where you can view and manage the incidents assigned to you.

Data Discovery Incidents

This section does not apply to Websense Web Security Gateway Anywhere.

Data Discovery Incidents displays the total number of data discovery incidents detected by a Websense Data Security discovery scan. Two graphs are included:

- **Top 5 Host Names:** displays the top 5 violating hosts and the number of incidents detected on these hosts broken into categories of urgency. (See above.)

- **Top 5 Policies:** displays the top 5 policy categories that were violated, and the number of incidents discovered for these policy categories.

The **Last data discovery incident** and **My data discovery incidents** fields work the same as for data usage incidents. (See above.)

Monitoring system health

The System Health screen enables you to monitor the performance of Data Security servers, protectors, and the Websense Content Gateway.

To view system health, select **Main > Status & Logs > System Health**.

The tree view displays the names of all protector appliances, Data Security servers, and, if installed, the Websense Content Gateway. Click a Data Security server or Websense Content Gateway to view the following charts in the right-hand part of the screen:

Chart	Description
System Summary	Information about the server, including operating system and version, time zone, and free disk space.
CPU Usage	The percentage of the CPU that is being used by the machine's processes over the specified time frame.
Memory Usage	The percentage of memory that is being used by the machine's processes over the specified time frame.

The System Summary and Memory Usage charts are also available for all protectors.

Data Security servers include the following modules in the tree view:

- PreciseID fingerprint repository
- Endpoint server
- Policy engine

Protectors and the Websense Content Gateway include the following modules:

- Policy engine
- PreciseID fingerprint repository

When you select a module, you view information about the system health and performance of that module. The right-hand part of the screen displays the statistics for events flowing through the system, enabling you to see how your system behaves with regards to traffic type (channels) and how busy the components are.

You can examine the following charts for each module:

Chart	Description
Protector	
Packet loss and dropped transaction indication	Indicates the levels of packet loss and dropped transaction rates.
Number of events sent to analysis	The number of events sent for analysis by this protector in the specified time frame.
Load average	Average amount of work performed by the protector in the specified time frame. For optimum performance, the number on the chart should not exceed the number of available processors in the System Summary: for example, if the system load average is 3 and there are 2 available processors, the system might work slowly.
Memory usage	The percentage of memory used by machine processes.
Total Throughput	Total amount of traffic (in KB per second) monitored by the protector. This includes both interesting and non-interesting sessions.
Data sent to analysis throughput	Total amount of traffic (in KB per second) sent for analysis by this protector.
Policy Engine	
Analysis status	Displays the request load on the policy engine for analysis by time period.
Data usage—number of analyzed events	Number of data usage events analyzed by this policy engine in the specified time frame.
Data usage—number of incidents	Number of data usage incidents detected by this policy engine in the specified time frame.
Data discovery—number of analyzed items	Number of data discovery items analyzed by this policy engine in the specified time frame. This includes files, email messages, and database tables. This chart is available only for policy engines on Data Security servers. If the policy engine on this computer does not handle discovery traffic, this report is empty.
Data discovery—number of incidents	Number of data discovery incidents detected by this policy engine in the specified time frame. This chart is available only for policy engines on Data Security servers. If the policy engine on this computer does not handle discovery traffic, this report is empty.
Fingerprint Repository	
Fingerprint repository synchronization	Displayed only on the Data Security Management server that contains the synchronization data. Shows the status of all fingerprint repositories, divided into time periods. The status for each time period indicates if a repository was fully synchronized with the main repository, required a partial synchronization, or required full synchronization.
Number of fingerprinted files	Displays the total number of files fingerprinted in the specified time frame.

Chart	Description
Number of fingerprinted database cells	Displays the total number of database cells fingerprinted in the specified time frame.
Endpoint Server	
Endpoint server load	Displays the load on the endpoint server over the specified time period.
Number of endpoints	Number of endpoint requests received by the endpoint server in the specified time frame.

For each chart, the **Display** drop-down list enables you to select a time frame for that chart. You can view statistics for the last 30 minutes, or the last 24 hours.

To download raw analysis data for troubleshooting purposes, click the **Download** button to the right of each chart.

For all modules, an **Advanced** section is also available. You can expand this section to view raw statistics supplied by the selected module.

You can use the information in these charts to fine-tune the system and optimize the performance of the Websense Data Security system.

Viewing endpoint status

Related topics:

- *Configuring endpoint settings*, page 290
- *Bypassing endpoint clients*, page 293

Websense data endpoints test their connectivity and check for configuration updates at time intervals specified in the endpoint system settings. The Endpoint Status screen summarizes the results of these checks. You can filter down to locate servers which have not synchronized or run data discovery for an extended period of time, and also view detailed information for a particular server.

To view the status of all installed Websense data endpoints:

1. Select **Main** > **Status & Logs** > **Endpoint Status**.

   The resulting screen lists all Websense data endpoints registered with the Data Security Management Server. The list displays information for each endpoint, such as:

   - Host name
   - IP address
   - logged-in users
   - last update time

- synchronization status
- discovery status (idle or running)

2. To drill down further on information for each endpoint, select an endpoint in the list and click the **More Details** pane. There you can view the profile name, fingerprinting version, and more.
3. To remove an endpoint from the list, select the endpoint and click **Remove**.

From this screen you can also do the following:

- Click **Settings** to view and edit the system settings for endpoint hosts. For more information, see *Configuring endpoint settings*, page 290.
- Click **Bypass Endpoint** to temporarily disable the selected data endpoint. For more information, see *Bypassing endpoint clients*, page 293.
- To search for a specific endpoint host in the list, in the **Find host** field enter the host name and click the **Find** button.

✓ **Note**

After an endpoint client receives an update and displays the new updated time, it can still take up to a minute until all policies are updated.

Viewing deployment status

Related topics:

- *Reviewing and deploying changes*, page 22

After you make changes to the policy configuration, you must click **Deploy** to deploy the changes in the network. Click the icon next to the **Deploy** button to view the status of the deployment. View the **Status** column for progress which can be one of:

- In progress
- Succeeded
- Failed

See *Troubleshooting* for tips on how to solve failed deployments.

Viewing logs

Related topics:

- *Traffic log*, page 204
- *System log*, page 205
- *Audit log*, page 206

The logs available in TRITON - Data Security enable you to analyze all events and actions in the manager, and to keep track of the traffic flowing through the Websense Data Security system.

There are 3 different logs you can view:

- *Traffic log*, page 204
- *System log*, page 205
- *Audit log*, page 206

Traffic log

The traffic log contains details of the traffic being monitored by Websense Data Security over specific periods. In this log you can see details of data that has breached policies, and the actions taken.

To view the contents of the traffic log, select **Main** > **System & Logs** > **Traffic Log**.

The **Updated to** field shows when the traffic log was last updated. To see the latest data, click **Update Now**.

Column	Description
Action Taken	The online action that was performed (permit or block).
Analyzed By	Displays the name of the server that analyzed the breach.
Classifier Time	Time spent analyzing all classifiers, in milliseconds. Includes the time spent processing dictionaries, scripts, key phrases, patterns, and fingerprints.
Channel	Channel on which the data was intercepted, for example SMTP, HTTP, or FTP.
Destination	The destination to which the data was sent.
Details	Further details of the data that breached a policy. For example, if the breach is in an email message, this column contains the message subject. If the breach was detected in an FTP transfer, this column lists the file name.
Detected By	Displays the protector or agent that caught the policy breach.

Column	Description
Event ID	Unique ID number of the event.
Event Time	Date and time the event occurred.
Extraction Time	Time spent extracting text from the transaction, in milliseconds.
Incident ID	Displays a check mark if the event was determined to be an incident (a policy violation).
Incident Creation Time	Time spent creating an incident when a breach is detected, in milliseconds. If no incident was created, this field is “0”.
Latency	Time the transaction spends in the policy engine waiting for analysis, in milliseconds—in other words, Processing Time + Incident Creation Time + Queue Time.
Prescribed Action	The name of the action plan that was triggered.
Processing Time	Time it took to process the event, in milliseconds—in other words, Classifier Time + Extraction Time + Resolution Time.
Resolution Time	Time spent resolving user names for all sources and destinations in the transaction, in milliseconds.
Size	The size of the data that was analyzed, for example a file or an email message.
Source	The source from which the data originated. This could be an email address or IP address or other source.

If one or more modules fails to provide updated traffic information, the **Errors detected** link appears above the traffic list. Click this link to open the Traffic Log Details screen and see the status of all modules and reasons for the update failure.

System log

The system log displays system actions sent from different Websense components, for example Data Security servers, protectors, or policy engines. You can examine the details of each action, including the date and time it occurred and the component that reported the action.

To view actions in the system log, select **Main** > **System & Logs** > **System Log**.

By default, the displayed actions are sorted by date and time. If a filter is used, the number of displayed actions is shown at the top of the list.

Column	Description
Severity	Defines whether the action is an error, or is reported for informational purposes.
Status	Displays either New or Confirmed. Once you view a new action, you can mark it as confirmed to show you’ve reviewed it. To mark a new action as confirmed, select the action and click **Mark as Confirmed**. To revert a confirmed action to new, select the event and click **Mark as New**.

Column	Description
Message	This column may contain variables that are filled by the system, for example a full folder path or a component name. If there are multiple identical messages in a short time interval, a combined message is displayed. TRITON - Data Security formats the messages so that the total number is displayed in brackets at the end of the message, for example “New component registered: XXX (2 messages in 5 sec.).”
Date & Time	Date and time the action occurred.
Local Date & Time	Date and time on the component where the action occurred.
Topic	Displays either System for system messages reported by system components, or Configuration for messages reported by the system after a configuration action is executed (usually by an administrator).
Reporter	Displays the system module’s name, for example Data Security Server - USA.
Component	Displays the internal component name, for example Policy Engine or Endpoint Server.

Audit log

The audit log displays actions performed by administrators in the system.

To view actions in the Audit Log, select **Main > System & Logs > Audit Log**.

By default, the displayed actions are sorted by date and time. If a filter is used, the number of displayed actions is shown at the top of the list.

Column	Description
ID	ID number of the action. You can quickly jump to an Audit Log action by entering the ID number in the **Find ID** field and clicking **Find**.
Date & Time	Date and time the action occurred.
Administrator	Name and user name of the administrator that initiated the action in TRITON - Data Security.
Access Role	Access role of the administrator.
Action Performed	Details of the action. This column may contain variables that are filled in by the system, for example an incident number or a component name.

Part III

Administering the System

11 Configuring System Settings

Related topics:

In Websense Data Security, many system settings are configurable. You can:

- Set preferences for incidents and reports
- Define parameters for exporting incidents to a file*
- Configure endpoint hosts*
- Configure user directory settings
- Configure remediation*
- Configure alerts
- Configure archive storage
- Enter subscription details
- Link data and Web security

*These options are not included with Websense Web Security Gateway Anywhere.

Access the system settings screens by selecting **Settings** > **Configuration** > **System**.

Setting preferences for incidents and reports

Related topics:

- *Viewing Incidents and Reports*, page 159
- *Setting general preferences*, page 210
- *Setting preferences for data usage incidents*, page 211
- *Setting preferences for data discovery incidents*, page 212

By going to **Main** > **Incidents & Reports**, you can view all of the incidents that Websense Data Security has discovered in your organization over time. On the **Settings** tab you can set preferences for those reports.

For example, for data usage incidents, you can define attachment size and forensics settings. For data discovery incidents, you can set database thresholds. You can also define general settings, like filtering and printing, that apply to all types of incidents.

To set preferences for incidents and reports:

1. Select **Settings** > **Configuration** > **System**.
2. Select the **Incidents & Reports** option from the System pane.
3. Complete the **General**, **Data Usage,** and **Data Discovery Incidents** tabs as described in the following sections.

Setting general preferences

To define general settings for security incidents and reports:

1. Select the **General** tab.
2. Complete the fields as follows:

Field	Description
Attachments	
Maximum number of attachments per message	Select the maximum number of report attachments (between 1-40) to append to each email notification message. By default, 40 attachments can be appended.
Maximum size of attachments	Select the maximum overall file size (between 1-20 MB) for the email notification message. By default, the maximum is 5 MB.
Zip incident and discovery reports	Select this box if you want to zip incident management and discover reports in an archive to minimize the size of the notification message.

Field	Description
Printing Incidents	
Printing Incidents	If a list of Websense Data Security incidents or reports gets very long, you can break it into groups for viewing and printing. Use this option to specify the number of incidents or reports to print at any one time. (This applies to both the **Print Preview** and **Export to PDF** functions.) Use the up/down arrows to choose a number between 50 and 500. (By default, incidents are printed in groups of 400.) If the total number of items to print is larger than the number you set here, you’ll be asked to select from a range of pages. For example, if you select 200 and there are 700 incidents, you’ll be asked if you want to print 1-200, 201-400, 401-600, or 601-700. If you prefer to print all incidents, you can enter an email address to which to send a PDF file.

3. Click **OK** to save your changes.

Setting preferences for data usage incidents

To define settings for reviewing data usage incidents:

1. Select the **Data Usage** tab.
2. Complete the fields as follows:

Field	Description
Web Mail Forensics	
Arrange the following fields at the top of the screen	Select this box if you want optional fields displayed in Incident & Reports screens. Type field names in the order you want to view them. (Separate multiple fields by commas.) For example: to, subject, body
View non-formatted data	Select this box if you want to include non-formatted data in Incident & Reports screen. For example: to, subject, subj, body, msgbody, plainmsg, cc, bcc, from, login.
Secure Forensics	
Indicate whether you want forensics to be secured	Select this box to block forensics from being displayed in potentially malicious HTML.

3. Click **OK** to save your changes.

Setting preferences for data discovery incidents

✓ **Note**
If you have Websense Web Security Gateway Anywhere, this section does not apply to you.

To define settings for data discovery incidents:

1. Select the **Data Discovery** tab.
2. Complete the fields as follows.

Field	Description
Maximum discovery incidents	Enter the maximum number (from 10,000-2,000,000) of incidents stored in the discovery database. (The Data Discovery Incidents screen enables assigning, viewing and monitoring these incidents.) Do not include commas.
Endpoint discovery incidents Network discovery incidents	Websense Data Security has a safety mechanism in place that protects the incident database from being overpopulated. When the same host, database, or mailbox generates many incidents for the same policy, the system quits storing incident details for each incident, and instead stores only general incident information. By default, 100,000 incidents must be generated for this change in behavior to take place. Indicate how many incidents you want to trigger the change. Do not include commas.

3. Click **OK** to save your changes.

Exporting incidents to a file

✓ **Note**
If you have Websense Web Security Gateway Anywhere, this section does not apply to you.

To export incidents to a log file for analysis:

1. Select **Settings** > **Configuration** > **System**.
2. Select the **Incident Export** option from the System pane.

3. Complete the fields as follows:

Field	Description
Export incidents to a file	Select this box to set up your incident export.
Path	Type the path where you want the incident report to be saved. Use the arrows to choose the maximum number (between 1-20) of log files you want to keep.
New file creation	Indicate how often you want to create a new incident export file.
When file size reaches	Click this radio button and select a file size (from 1-5MB) to create a new incident report file when the old file exceeds your specified size.
At the start of a new day	Click this radio button to create a new incident log file at 12:00 a.m. every day.

4. Click **OK** to save your changes.

Listed below are the fields that are exported and a description of their contents.

Field	Description
Incident ID	External incident ID.
Insert date	The incident insert date.
Source host name	The incident source host name.
Source IP	The incident source IP.
Source full name	The incident source full name.
Source email	The incident source email.
Source DN	The incident source DN.
Destinations list	A list of the incidents destinations, in the format of dest1;dest2;dest3…
Channel name	The channel name.
Max action taken	A readable action taken (e.g.: Blocked, Audited).
Urgency	Incident’s urgency, sometimes called sensitivity (e.g.: Moderate).
Policy category	A policy category for the current line (an incident can generate multiple lines).
Filenames	The filename(s) related to the current incident policy, up to 1024 characters. In the format of [fn1;fn2;…;fnX].
Filenames trimmed	True if the actual value for the filenames filed is greater than 1024 characters. Please notice that in few cases you do not get the actual file name. For example, for some SMTP incidents you might see the filename as MESSAGE-BODY.

Field	Description
Breached contents	The breach content of the incident for the current policy, up to 1024 characters, in the format of [content1;content2;…;contentX].
Breached content trimmed	True if the actual size of the previous filed is more than 1024 characters.

Configuring endpoints

Related topics:

- *Configuring Endpoint Deployment*, page 281
- *Endpoint Devices*, page 109
- *Endpoint Applications*, page 109
- *Endpoint Application Groups*, page 110

✓ **Note**

This section applies only to customers with Websense Data Endpoint. If you have Websense Web Security Gateway Anywhere, it does not apply to you.

In this section, you can configure parameters for endpoints, such as how often to test connectivity and check for updates, how much disk space to use for system files, and the action to take when user confirmation is required but not attained.

1. Select **Settings** > **Configuration** > **System**.
2. Select the **Endpoint** option from the System pane.
3. Complete the fields as follows:

Field	Description
Connectivity	
Test connectivity every	Select how often (between 1-60 minutes) endpoints test connectivity. Default is 5 minutes.
Check for updates every	Select how often (between 1-24 hours) endpoints check for configuration updates. Default is 1 hour.
An endpoint is disconnected if no signal is received within	Define when (between 1-60 hours) the endpoint is determined to be disconnected. Default is 5 hours.
Disk Space	
Maximum log file size	Limit the size (between 16-100 MB) of the endpoint client’s log file. Default is 16MB.

Field	Description
Incident storage allocation	Specify the incident-storage disk space to allocate (between 10-100 MB) for disconnected endpoints.
PreciseID fingerprint storage	Specify the disk space (between 1-1000 MB) to allocate for storage of directory and SharePoint fingerprints.
Other	
Action	Select an action consequent to a user policy breach when no default action has been specified. (Options are **Block** or **Permit**.)
Endpoint Administrator Password	Provide and confirm a password for administering endpoint clients. This helps prevent users from uninstalling or tampering with the Websense Data Security system.

4. Click **OK** to save your changes.

Configuring user directory settings

Related topics:

- *Adding a new user directory server*, page 215
- *Rearranging user directory servers*, page 217
- *Importing users*, page 217
- *Importing user entries from a CSV file*, page 218

In Websense Data Security, you can import user, group, and computer information from user directory servers, such as Microsoft Active Directory or Lotus Domino servers. This prevents you from having to add such information manually, and guarantees that the most updated information is available.

To take advantage of this feature, you need to set up your user directory server(s) and schedule user directory synchronization.

To configure user directories:

1. Select **Settings** > **Configuration** > **System**.
2. Click the **User Directories** option in the System pane.

You can add a new directory server, delete an existing directory server, rearrange servers according to priority, or import user information.

Adding a new user directory server

1. Click **New** in the User Directory Servers toolbar.

2. Complete the fields as follows:

Field	Description
Name	Enter a name for the user directory server.
Type	Select the type of directory from the pull-down menu: Active Directory, Domino, ADAM, or CSV file. If you choose CSV, you must set up your CSV files in a certain format. Refer to *Importing user entries from a CSV file*, page 218 for details.
Follow referral	Select this option if you want Websense Data Security to follow server referrals, should they exist. A server referral is when one server refers to another for programs or data. Select **Ignore Referral** if you don't wish to follow such referrals. Referrals are an LDAP feature that gives you the ability to build hierarchies of LDAP servers. Follow referrals with caution. If not set up properly, referred queries can take a long time and appear to be time-outs.
Connection Settings	
IP address or host name	Enter the IP address or host name of the user directory server.
Port	Enter the port number of the user directory server.
User name	Enter a user name that has access to the directory server.
Password	Enter the password for this user name.
Use SSL Connection	Select this box if you want to connect to the directory server using Secure Sockets Layer (SSL) encryption.
Test Connection	Click this button to test your connection to the user-directory server.
Directory usage	
Import user records from this server	Select the **Import user records from this server** check box if you plan to import user records from this server. This enables the user directory and places it on the resources page (**Main > Policy Management > Resources > Directory Entries**). If you do not select this check box, you cannot add these resources to your policies.
Get additional user attributes	Select this box if you want to retrieve user information from the directory server.
Attributes to retrieve	Enter the user attributes that you want TRITON - Data Security to collect for all users. Separate attributes by commas. For example: title, manager, department.
Sample email address	Enter a valid email address with which you can perform a test.

Field	Description
Test Attributes	Click **Test Attributes** to retrieve user information on the email address you supplied. Click **View Results** to check the imported user information.
Use this server to authenticate logged-in administrator	Select this option if you want to authenticate administrators on this server when they log on to Websense Data Security.

3. Click **OK** to save your changes.

Rearranging user directory servers

The order of your user directory servers is important, because users are imported from directories in the listed order. If a user exists in more than one directory, the first record in the directories takes precedence.

To define the ranking your user directory servers:

1. Select **Settings** > **Configuration** > **System**.
2. Click the **User Directories** option in the System pane.
3. Click **Rearrange Servers** in the toolbar.
4. In the rearrange User Directory Servers dialog box, click individual server names and use the up/down arrows to promote or demote the servers to the desired order.
5. Click **OK** to save your changes.

Importing users

You can import user data immediately from a directory or schedule the import.

1. Select **Settings** > **Configuration** > **System**.

2. Click the **User Directories** option in the System pane.

Field	Description
Import Now	Click the **Import Now** button to immediately import user information in the server list order. (It can take some time to perform this action. A confirmation screen appears.)
Import daily at [3:00 a.m.]	The **Import daily at [3:00 a.m.]** link indicates the current schedule for user directory imports. The time shown in the square brackets [ ] may vary. Click this link to adjust the import schedule. Use the up/down arrows to set the desired import time. Click **OK** to save changes.

✓ **Note**

Imports from CSV files cannot be scheduled. You must click **Import Now** to import data from a CSV user directory.

Importing user entries from a CSV file

User directories can be in comma-separated values (CSV) files. You have the option to import user directory entries from such files. To do that, you must generate a set of files in a specific structure.

1. Create 3 text files named **computers.csv**, **users.csv**, and **groups.csv**. See *CSV file formatting* for details on the format.
2. Click **New** in the User Directory Servers toolbar.
3. Select **CSV File** in the Type field.
4. Enter the path of the CSV files.
5. Click **OK**.
6. Each time you want to import user, group, or computer data from the CSV files, go to **Settings** > **Configuration** > **System** > **User Directories** and click **Import Now** on the menu bar. For CSV directories, you cannot schedule automatic synchronization.

CSV file formatting

When you create your CSV user directory files, ensure that these conditions are met:

- Encoding:

  Use the UTF-8 character set or use a character set that is supported by its JVM installation.
- Separate fields using commas.
- End each record with a line feed or carriage return/line feed.

- Escaping and quotes:
    a. Enclose fields that contain a special character (semicolon, new line, or double quote) in double quotes.
    b. If a field's value contains a double-quote character, escape it by placing another double-quote character next to it.
- Omit optional fields and replace them with the delimiter.
- When a field contains a list, separate the list elements using a semicolon (;) and enclose the entire field in double quotes, unless the list contains one element or none.

Groups file format

Each row in the **groups.csv** file should contain:

Name	Data Type	Optional	Description
UUID	String	No	The record's universal unique identifier
Name	String	No	Group name
Description	String	Yes	Description
memberOf	List of UUID	Yes	UUIDs of which this group is a member (can be empty)

For example:

```
08b3b46b-3631-46cb-adc7-176c2871e94c,Marketing - EMEA,
Marketing department,7c9d4db6-1737-4b80-9e6e-42f415300a05

40632a33-db39-4f93-bd80-093e0b3230ca,Marketing - APAC,
Marketing department,7c9d4db6-1737-4b80-9e6e-42f415300a05

7c9d4db6-1737-4b80-9e6e-42f415300a05,Marketing all,All
Marketing departments
```

Users file format

Each row in the **users.csv** file should contain:

Name	Data Type	Optional	Description
UUID	String	No	The record's universal unique identifier
Name	String	No	User name
Email	String	Yes	Email address (primary)
Description	String	Yes	Description
managerUUID	String	Yes	UUID of the current user's manager

Name	Data Type	Optional	Description
memberOf	List of UUID	Yes	UUIDs of which this group is a member (can be empty)
Zero or more “additional attributes” fields	String	Yes	See “Additional Attributes” below

Additional attributes

User records can have additional attributes attached. The additional attributes are name value pairs containing information that you might want attached to users. Some of these attributes have predefined names (see below). A file containing an additional attribute should be defined as a regular expression of the following format:

```
[aA][tT][tT][rR]:(.+)/=/(.+)
```

You can choose to use any name you wish for custom attributes; they will be stored as an associated array on the user object and are used only for display. However, the following includes a well-known list of attribute names:

- wbsn_proxy_address - secondary (alternative) email address
- wbsn_login_name - the user login name (principal name on Windows-based systems)
- wbsn_full_name - the user’s display name
- wbsn_department - department
- wbsn_telephone_number - the user’s telephone number
- wbsn_title - the user’s title
- wbsn_mailbox_store - the server on which the user’s Exchange mailbox is stored

The table below illustrates some attributes:

String	Name	Value
attr:wbsn_title/=/Manager	wbsn_title	Manager
aTTr:my amazing attr/=/the value	my amazing attr	the value
“ATTR:name/=/value1,value2”	name	value1,value2

For example:

```
6278ab76-2ce2-4f16-8e49-aa5104da7d0b, jdoe-mgr,
jdoe.manager@example.com,CEO,7c9d4db6-1737-4b80-9e6e-
42f415300a05,attr:room/=/201,attr:parkingSpace/=/1

ff255105-4e43-4e9a-b2bd-e366872cd212, jdoe,
jdoe@example.com, administrator, 6278ab76-2ce2-4f16-8e49-
aa5104da7d0b,"08b3b46b-3631-46cb-adc7-176c2871e94c;7c9d4db6-
1737-4b80-9e6e-42f415300a05",attr:room/=/101
```

Computers file format

Each row in **computers.csv** should contain:

Name	Data Type	Optional	Description
UUID	String	No	The record's universal unique identifier
Name	String	No	Computer name (host name)
FQDN	String	Yes	DNS fully qualified domain name
Description	String	Yes	Description
memberOf	List of UUID	Yes	UUIDs of which this group is a member (can be empty)

For example:

```
379a287f-0a5c-40ff-85fd-fae3da462d03,gumby,
gumby.example.com, print server,"7c9d4db6-1737-4b80-9e6e-
42f415300a05"
```

Configuring remediation

Related topics:

- *Remediation*, page 112

✓ **Note**

If you have Websense Web Security Gateway Anywhere, this section does not apply to you.

To define the location of the syslog server and mail release gateway used for remediation:

1. Select **Settings** > **Configuration** > **System**.
2. Click the **Remediation** option in the System pane.

Field	Description
Syslog Settings	
IP address or host name	Enter the IP address or host name for the syslog server.
Port	Enter the port number for the syslog server.

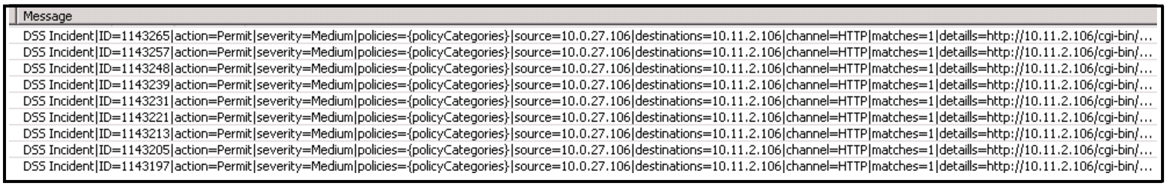
Field	Description
Use syslog facility for these messages	Select this box to see the origin of syslog messages. Use the drop-down menu to select the type of message that will appear in the syslog.
Test Connection	Click **Test Connection** to send your syslog server a verification test message
Release Gateway	
IP address or host name	Enter the IP address or host name for your mail release gateway. The mail release gateway is used to deliver email messages that were blocked and subsequently released.
Port	Enter the port number for your mail release gateway.

3. Click **OK** to save your changes.

The syslog message includes the following information for each incident:

- incident ID
- action taken
- severity assigned
- policies affected
- incident source
- incident destination
- channel
- number of matches
- details

For example:



```
Message
DSS Incident|ID=1143265|action=Permit|severity=Medium|policies={policyCategories}|source=10.0.27.106|destinations=10.11.2.106|channel=HTTP|matches=1|detaills=http://10.11.2.106/cgi-bin/...
DSS Incident|ID=1143257|action=Permit|severity=Medium|policies={policyCategories}|source=10.0.27.106|destinations=10.11.2.106|channel=HTTP|matches=1|detaills=http://10.11.2.106/cgi-bin/...
DSS Incident|ID=1143248|action=Permit|severity=Medium|policies={policyCategories}|source=10.0.27.106|destinations=10.11.2.106|channel=HTTP|matches=1|detaills=http://10.11.2.106/cgi-bin/...
DSS Incident|ID=1143239|action=Permit|severity=Medium|policies={policyCategories}|source=10.0.27.106|destinations=10.11.2.106|channel=HTTP|matches=1|detaills=http://10.11.2.106/cgi-bin/...
DSS Incident|ID=1143231|action=Permit|severity=Medium|policies={policyCategories}|source=10.0.27.106|destinations=10.11.2.106|channel=HTTP|matches=1|detaills=http://10.11.2.106/cgi-bin/...
DSS Incident|ID=1143221|action=Permit|severity=Medium|policies={policyCategories}|source=10.0.27.106|destinations=10.11.2.106|channel=HTTP|matches=1|detaills=http://10.11.2.106/cgi-bin/...
DSS Incident|ID=1143213|action=Permit|severity=Medium|policies={policyCategories}|source=10.0.27.106|destinations=10.11.2.106|channel=HTTP|matches=1|detaills=http://10.11.2.106/cgi-bin/...
DSS Incident|ID=1143205|action=Permit|severity=Medium|policies={policyCategories}|source=10.0.27.106|destinations=10.11.2.106|channel=HTTP|matches=1|detaills=http://10.11.2.106/cgi-bin/...
DSS Incident|ID=1143197|action=Permit|severity=Medium|policies={policyCategories}|source=10.0.27.106|destinations=10.11.2.106|channel=HTTP|matches=1|detaills=http://10.11.2.106/cgi-bin/...
```

Configuring alerts

Related topics:

- *Setting general alert preferences*, page 223
- *Setting up email properties*, page 223
- *Editing outgoing mail server properties*, page 224

In the system settings, you can define when you want to trigger alerts and whether the alerts should be sent to the syslog or emailed to an administrator. If an alert is to be sent by email, you can define the sender, recipient(s), subject, and mail server.

1. Select **Settings** > **Configuration** > **System**.
2. Click the **Alerts** option in the System pane.
3. Complete the **General** and **Email Properties** tabs as described in the following sections.

Setting general alert preferences

Use the check boxes to select when you want to trigger alerts, such as when your subscription is about to expire. You can send email alerts when:

- Your subscription is about to expire
- The number of discovery incidents reaches its limit
- The archive disk space reaches its limit
- The forensics disk space reaches its limit
- A new administrator is added to TRITON - Data Security

Setting up email properties

To define properties for alerts that are sent by email:

1. Click the **Email Properties** tab.
2. Complete the fields as follows:

Field	Description
Sender name	When an alert notification is sent to administrators, from whom should the report be coming?
Sender email address	Enter the email address of the person from whom the notification will be coming.
Subject	Enter the subject line for the scheduled alert notifications.
Recipients	Click **Edit** to select the recipients to whom alerts should be sent. You'll see a Directory Entries window with searchable and selectable recipients. Click **OK** to save your changes. To add one or more further recipients, select **Additional email addresses**, then enter the address(es) of the recipient(s). Use commas to separate multiple email addresses.

3. Click **OK** to save your changes.

Editing outgoing mail server properties

1. To define or edit the **Outgoing mail server**, click the pencil icon. Complete the fields as follows:

Field	Description
IP address or host name	Enter the IP address or host name of the outgoing SMTP mail server to use for scheduled alert notifications.
Port	Enter the port number of the mail server to use. Click **OK** to save your changes.

2. Click **OK** to save your changes.

Configuring archive storage

To define storage location and size:

1. Select **Settings** > **Configuration** > **System**.
2. Click the **Archive Storage** option in the System pane.
3. Complete the fields as follows:

Field	Description
Store archive locally	Select this radio button if you want to store the incident archive on the local machine.
Archive folder	Enter the path for your local archive folder. By default, the archive is stored in a local folder under %DSS_HOME%.
Maximum archive disk space	Enter the maximum amount of disk space you want allocated for archive storage.
Store archive remotely	Select this radio button if you want to store the incident archive on a remote machine in your network.
Use existing storage location	Use the drop-down menu to select a previously configured storage location. Click **Delete** to remove unneeded locations.
Name new storage location	Select this radio button to define a new storage location. Enter a name for the new location.
IP address or host name	Enter an IP address or host name for the machine on which the storage will be located.
Domain	Enter the domain name.
User name	Enter the user name needed for location access.
Password	Enter the password needed for location access.
Archive folder	Type in the path to the new archive folder.

Field	Description
Test Connection	Click **Test Connection** to make sure the Data Security server can access the storage location.
Description	If desired, enter a description for the archive location.
Maximum archive disk space	Select a limit on the storage drive for disk space used by the archive.

4. Click **OK** to save your changes.

Entering subscription settings

Related topics:

◆ *Subscription alerts*, page 226

To enter subscription details for the first time:

1. Log onto TRITON - Data Security. If you have never entered subscription information before, the subscription page appears automatically.
2. Select the module to which you subscribe:
   - Websense Data Security
   - Websense Web Security Gateway Anywhere
3. If you select Websense Data Security, browse to your subscription file, then click **Submit**. Your subscription terms are displayed, including the start and expiration dates, the number of subscribed users, and the modules to which you subscribe. The TRITON - Data Security application restarts.

If you have Websense Web Security Gateway Anywhere, your subscription key should be entered in TRITON - Web Security or Content Gateway Manager. This information is communicated to Websense Data Security automatically.

When you purchase an upgrade or change your subscription type, you must update your Websense Data Security subscription file. If you do not, an error message displays when you try to use Websense Data Security.

To update your Websense Data Security subscription:

1. Select **Settings** > **Configuration** > **System**.
2. From the System pane, choose **Subscription**. Your current subscription terms are displayed.
3. Click **Update** on the toolbar.
4. Browse to the new subscription file, then click **OK**. The TRITON - Data Security application restarts automatically.

Subscription alerts

The system alert summary on the Websense Data Security Today page alerts you when your subscription is about to expire. These alerts start 30 days before expiration; the message in the summary section states that the subscription is about to expire in X days.

In addition, system administrators receive an email message stating that the license is about to expire 30 days before the expiration, and then once a week until it expires.

Popup messages stating that the license is about to expire are also displayed to all administrators that have access to the settings when they log on.

Warning

Once a subscription expires, traffic is no longer analyzed. This means that violations of your policies are not monitored or blocked.

When the license expires there is a 2-week grace period, after which the system stops analyzing data. After the license expires, you can:

- access old incidents
- access reports
- access configurations and make changes
- deploy settings

To renew or purchase a subscription, contact a Websense Data Security sales representative.

Linking data and Web security

Related topics:

- *Enabling joint administration*, page 228
- *Importing URL categories*, page 228
- *Editing Linking Service properties*, page 229

This section describes how to link Websense Data Security with Websense Web Security and enable the Websense Linking Service.

Linking is designed for organizations with Websense Web Security. It provides 2 benefits:

- It gives administrators access to TRITON - Web Security and TRITON - Data Security from the same unified console. (Identical administrator credentials must be configured in both managers for this to work.)
- Access to the *Websense Linking Service* that was installed with Websense Web Security. The Websense Linking Service provides IP address to user name resolution for HTTP incidents. With this service, Websense Data Security is able to display user names in incident reports rather than IP addresses.

  In addition, the Linking Service allows Websense Data Security to import Web Security's preset and custom URL categories so you can add them as resources in your DLP policies.

To configure linking:

1. Select **System Tools** > **Configuration** > **Settings**.
2. From the System pane, choose **Linking**.
3. Enter the IP address and port as follows:

Field	Description
IP address or host name	Enter the IP address or host name of the TRITON - Web Security machine (also known as the Web Security Manager machine).
Port	Enter the port number of the TRITON - Web Security machine.

4. Click **Link**. This creates a connection between TRITON - Data Security and TRITON - Web Security.

   When you click **Link**, TRITON - Data Security looks for the Websense Linking Service and enables it. It displays the IP address and port number for the Linking Service that it found in the Linking Service section of the screen. (Note that these settings change frequently. If you need to edit the IP address for any reason, refer to *Editing Linking Service properties*, page 229.)
5. Click **Test Connection** to test the linking connection. A confirmation message is returned.
6. Click **OK**.

Now that linking is established, do the following:

1. Enable the buttons in the module tray. See *Enabling joint administration*, page 228 for instructions.
2. Import URL categories from the Websense Master Database. See *Importing URL categories*, page 228 for instructions.

You can also configure linking through Websense Web Security. In TRITON - Web Security, select **Settings** > **General** > **Linking** to access configuration settings**.** It's not necessary to configure linking in both modules. Websense Data Security administrators are notified if linking is activated in Web Security.

Note

If you have trouble configuring linking, accessing one module from another, or using the buttons in the TRITON module tray, see the troubleshooting topic, *Linking*, page 309.

Enabling joint administration

Related topics:

- *Defining administrators*, page 231
- *Adding a new administrator*, page 232

If you want the buttons in the TRITON module tray to become active for administrators—in other words, you want them to be able to click Web Security button to access TRITON - Web Security—you must ensure that they have accounts in both the Web and data security modules with the same user names and passwords.

If you are new to Websense Data Security, create administrator accounts in TRITON - Data Security with the same user names and passwords as the accounts you have in Web Security. If you are new to Websense Web Security, create accounts in TRITON - Web Security that match the accounts you have in Data Security.

The accounts can be local accounts or user directory accounts, as long as the user names and passwords are the same.

See *Defining administrators*, page 231 for instructions on creating administrator accounts in TRITON - Data Security.

See “Delegated Administration” in the TRITON - Web Security help for instructions on creating administrators in TRITON - Web Security.

Importing URL categories

Related topics:

- *URL categories*, page 107
- *Rule Wizard - Source*, page 58
- *Rule Wizard - Destination*, page 59

The Websense Linking Service that became enabled when you configured linking provides access to the URL categories in the Websense Master Database. To import these categories:

1. Select **Main > Resources > URL Categories**.
2. Click **Update Now** in the toolbar.

The category list populates with all available URL categories. Update this list periodically, as the categories change frequently.

Now you can select a URL category or categories as sources or destinations in your policy rules.

Editing Linking Service properties

Normally you should not need to edit Linking Service properties. The data and Web security modules communicate regularly to update the location of the service.

If you want to change the properties for the Linking Service—for example, if it stops responding—access the Linking screen and click **Edit** under Linking Service.

Here you can disable the service or retrieve the latest IP address and port number for the service. To do the latter, click **Update**. (You can also enter this information manually.) The information on the screen updates if the settings are retrieved successfully.

Click **Test Connection** to test the connection to the Linking Service. A confirmation message is returned.

Note that if you click **Remove Link** to disconnect Data and Web Security servers, the Linking Service is automatically disabled.

12 Configuring Authorization

Related topics:

- *Defining administrators*, page 231
- *Working with access roles*, page 233
- *Configuring personal settings*, page 236

Select **Configuration** > **Authorization** on the **Settings** tab to configure authorization for your data security system. This section of TRITON - Data Security lets you:

- Define administrators - the people who manage the data security system
- Set up access roles - such as the Superuser, Administrator, and Log Auditor. Each role has different permissions
- Configure personal settings - view and change passwords or restore reminders

Defining administrators

Related topics:

- *Adding a new administrator*, page 232

Important

You must define at least one administrator in order to use the system. By default, the first administrator has Superuser privileges.

Websense Data Security administrators configure security policies, view incidents, fine-tune system performance, and more. You may have one Superuser in your system, or you may have multiple administrators with different responsibilities.

To view or define the users who administer your data security system:

1. Select **Settings** > **Configuration** > **Authorization**.
2. Click the **Administrators** option in the Authorization pane.

   The resulting screen lists all the administrators that have been defined, along with their user names, user information source, access roles, and permissions.
3. Click a user name to view or edit an administrator profile, or click **New** to add a new administrator.
4. To delete an administrator, select it, then click **Delete**.

Adding a new administrator

Related topics:

◆ *Working with access roles*, page 233

To define a new system administrator:

1. Click **New** on the Administrators page menu bar.
2. Select the source of user information for this administrator:
   - Select **User directory** if you want to add administrator details through an LDAP directory service such as Active Directory.
   - Select **Local** if you want to add administrator details manually.
3. Add user details for this administrator.

   If you chose **User directory**, enter the administrator's email address and click **Import User Details**. The user name and password for this user are imported.

   If you chose **Local**, enter a user name for this administrator, as well as an email address and password. (There are no password limitations.)
4. Add an optional description for this administrator.
5. Select an access role for this administrator from the drop-down list. There are several default access roles to choose from, or you can click **New** to create a new role. Click **View Permissions** to view the permission settings for the access role you choose.
6. Select which policies and business units the administrator can view. This affects what incidents he can manage.
   - Select **None** if you want this administrator to manage no policies at all, only assigned incidents.
   - Select **Customized** to select which policies and business units the administrator can access. If you select **Customized**, then choose either **All** or **Selected** policies and business units.
     - If you choose **All**, all current and future policies and business units (and their incidents) are accessible to this administrator.

- If you choose **Selected**, check the specific policies and business units this administrator can access. Choosing **Select All** selects all the items listed in the current window, but future policies or business units are not selected.

> ✓ **Note**
>
> Business Units applies only to data usage incidents. All administrators can view discovery incidents from all business units.

7. Click **OK** to save your changes.

An email message is sent to the new administrator with log on details. If the administrator has a local account, a password is provided. The administrator is asked to change the password when logging on for the first time.

Working with access roles

You may have several different administrators in your system. One may be responsible for installing and deploying system components. Another may configure and fine-tune security policies. And a third may view and respond to incident logs and reports. Each of these administrators may need access to different system functions, with only the Superuser requiring access to all.

This is where *access roles* come into play. Access roles define the access privileges for various administrative roles in your organization. By default, the following access roles are defined:

- **Superuser -** can access all configuration and management screens with read and write privileges
- **System Administrator -** can access the system settings functions, the deployment options, and the Status & Logs screens.
- **Policy Manager -** can configure policies, qualify and assign incidents.
- **Incident Manager -** can access incidents that were assigned to him/her and manage incident handling for those incidents.
- **External Auditor -** can view incidents and reports and some Status & Logs screens.

You can edit access privileges for these default roles or you can add new access roles. You can then assign an access role to each of your system administrators.

1. Select **Settings** > **Configuration** > **Authorization**.
2. Click the **Access Roles** option in the Authorization pane.

   The resulting screen lists all the access roles that have been defined, along with the permissions set for the roles and descriptions.
3. Click a name to edit a role or click **New** to define a new access role.
4. To delete an access role, select it then click **Delete**.

Adding a new access role

Related topics:

- *Adding a new administrator*, page 232

To define a new access role:

1. Click **New** on the Access Roles page toolbar.
2. Complete the fields as follows. Note that items marked with an asterisk do not apply to Websense Web Security Gateway Anywhere customers.

Field	Description
Name	Enter a name for the new access role
Description	Enter an optional description for the role
Permissions	Select **Full Control** if you want to give this role complete access to system functions Select **Customized** if you want to selectively define the reach of this role into your system.

Field	Description
Incidents & Reports	Select the incident and reporting functions that this access role should be able to access. **Data Usage** ◆ **Summary reports** - Select this option to give administrators with this role access to data usage summary reports. ◆ **Detail reports** - Select this option to give administrators with this role access to data usage detail reports. When this option is selected, several more are made available: • **View violation triggers** - Select this option if you want the administrator to view the values that trigger violations. • **View incident data** - Select this option if you want the administrator to view forensics for this incident. (Users who aren’t allowed to see this confidential data cannot see a preview of the email message or the content of the transaction in other channels.) • **Hide source and destination** - Select this option if you want to display identification numbers instead of source and destination names. Leaving this unchecked displays source and destinations as names. • **Perform operations on incidents** - Select this option if you want administrators with this role to be able to perform all escalation, remediation, and workflow operations on data usage incidents. **Data Discovery*** ◆ **Summary reports** - Select this option to give administrators with this role access to data discovery summary reports. ◆ **Detail reports** - Select this option to give administrators with this role access to data discovery detail reports. When this option is selected, more are made available: • **View violation triggers*** - Select this option if you want the administrator to view the values that trigger discovery violations. • **Perform operations on incidents*** - Select this option if you want administers with this role to be able to perform all escalation, remediation, and workflow operations on data discovery incidents. Check the **Send email notifications** box if you want email reports of incidents sent to this administrative role.
Policies	Select either or both of the **Data usage** and **Data discovery*** boxes to give this role access to these policy management pages. Administrators with access to the data usage pages can configure data usage policies, content classifiers, and resources. Administrators with access to the data discovery pages can configure data discovery policies, tasks, content classifiers, and resources.

Field	Description
Status & Logs	Select the status reports and logs to which this role should have access: ◆ The **Today** page shows system alerts, statistics, and an incident summary over the last 24 hours. ◆ The **System Health** screen enables you to monitor the performance of Data Security servers and protectors. ◆ The **Endpoint Status*** screen summarizes the results of endpoint connectivity tests. ◆ The **Traffic log** contains details of the traffic being monitored by Websense Data Security over specific periods, such as data that has breached policies and the actions taken. ◆ The **System log** displays system events sent from different Websense components, for example Data Security servers, protectors, or policy engines. ◆ The **Audit log** displays actions performed by administrators in the system.
Configuration	Select which options in the Configuration area of the **Settings** tab administrators with this access role should be able to access. **System** - System administrators can set up file and server locations for Websense Data Security functions, define preferences and activate subscriptions **Authorization** - Administrators can configure Websense Data Security authorization settings. **Archive** - Administrators can select incident partitions, then archive, restore or delete them. Regardless of selection, administrators can always change their passwords.
Deployment	Select which functions administrators with this access role should be able to perform. **Manage system modules** - Give this role the ability to register modules with the Data Security Management Server. **Manage endpoint profiles*** - Give this role the ability to view and edit endpoint profiles. Administrators can add new endpoint profiles, delete profiles, and rearrange their order. **Deploy settings** - Give this role the ability to deploy configuration settings to all system modules.

3. Click **OK** to save your changes.

Configuring personal settings

To configure personal settings, such as passwords and reminders:

1. Select **Settings** > **Configuration** > **Authorization.**
2. Select the **My Settings** option on the Authorization pane.

3. Complete the fields as follows:

Field	Description
Restore Reminders	
Show all reminders	Select this box if you want to restore reminders that you have previously marked “Do not show this window again.” This includes the reminder that deployment is needed.
Change Password	
User name	Your user name (uneditable)
Old password	Enter your old password
New password	Enter a new password. It cannot be a password you’ve used in Data Security before. There are no limitations on the characters the password can contain.
Confirm new password	Enter the new password again.

4. Click **OK** to save your changes.

13 Archiving Incidents

Related topics:

- *Archiving a partition*
- *Restoring a partition*
- *Deleting a partition*, page 242
- *Viewing Incidents and Reports*, page 159

TRITON - Data Security keeps a dynamic tally of incidents, which are automatically saved in a partition dubbed the *Online-Active* partition. Once full, that partition becomes inactive, replaced by a new active partition in order to maintain free storage for future forensics records. You can view and manage these partitions through TRITON - Data Security.

Select **Settings** > **Configuration** > **Archive** to view a list of current partitions and their status. You can archive, restore, or delete a partition, and also set storage limits using buttons on the toolbar.

In the Archiving screen, the bolded first line is the active partition. You cannot archive this partition, and if you delete it, its incidents are cleared but the partition is not removed. Event partitions represent roughly 3 months, and hundreds of thousands of incidents that have traversed the data security software. You can have a maximum of 8 online partitions (approximately 2 years), or 750,000 incidents. You can archive up to 12 partitions, which represents 3 years of records.

The columns in the archive list are sortable.

Column	Description
ID	An internally set identifying number beginning with the year. Click the incident partitions to select them for archiving.
Status	The current status: • **Online-Active** - local incidents are dynamically stored here until the repository is full • **Online** - once the Online-Active partition is full, a new Active partition begins to collect new incidents. The original Active partition is no longer active, but is retained here with its Online status. • **Archive** - partitions that have been archived in an offline location. • **Deleted** - partitions that have been permanently deleted. **Restored** - partitions that were restored to Online from having been archived.
From Date	The first event logged in the archive.
To Date	The last event logged in the archive.
# Incidents	The number of incidents currently collected in the archive.
Archive Storage	The location of the archive, whether local or at an external IP address.
Archive Path	The complete path to the external storage.
Comments	You can add optional comments about the archive in this field.
Show deleted partitions	Select this box to display deleted partitions in the Archiving list.

Toolbar buttons

You can select partitions and then archive, restore, or delete them by clicking the respective buttons in the toolbar:

Button	Icon	Description
Archive	🗂	Click this button to send a selected archive to offline storage. *Archiving a partition*, page 241
Restore	🗂	Click this button to restore a selected archived partition. *Restoring a partition*, page 241
Delete	✗	Click this button to delete a selected partition. Note: partitions are permanently deleted. *Deleting a partition*, page 242
Settings	🔧	Click this button to go to a screen where you can define the archive size and the storage location. *Archiving Incidents*, page 239

Archiving a partition

Incident partitions will automatically fill, but you can only keep 8 partitions online. If you want to save older partitions, you can archive them offline. The maximum local offline storage allowed is 12 partitions (approximately 3 years of records). To archive a partition:

1. Select the desired incident partition(s) in the Archiving screen.
2. Click **Archive** in the toolbar.
3. Review the list of partitions to be archived, adding comments if desired.

Field	Description
Year	The year the partition was created
Partition	The number of the partition to be archived
Status	The current status—Online-Active, Online, Archive, Deleted, Restored (for partitions that were restored to Online from Archive)
From Date	The first event logged in the partition
To Date	The last event logged in the partition
Archive Location	The location of the archive, whether local or at an external IP address
Archive Folder	The complete path to the external storage
Comments	You can add optional comments about the archive in this field

4. Click **OK** to continue.

The number of partition archives you can create depends on the size of the partition location.

Restoring a partition

You may want to restore archived partitions, if for example, you wanted to compare older incident patterns with newer ones. The maximum restored storage allowed is 8 partitions (approximately 2 years of records). To restore incident partitions from their archives:

1. Select **Settings** > **Configuration** > **Archive**.
2. Select the partitions of interest using their check boxes.
3. Click **Restore** in the toolbar.
4. You’ll see a “Selected archive partitions were successfully restored” confirmation dialog.
5. Click **OK**.

The Status line for the restored partitions indicates their restoration.

✓ **Note**

Before restoring an archive, the repository checks to see how much disk space is consumed by the restore operation. If restoration exceeds 95 percent of the allowed disk space, you cannot perform the restore. Once you've successfully completed the restore, the archived records should be deleted from the archive folder.

Deleting a partition

The archiving tools let you delete partitions.

1. Select **Settings** > **Configuration** > **Archive**.
2. Select the partitions of interest.
3. Click **Delete** in the toolbar. A summary of the partitions to be deleted appears. If one of the partitions is active, a warning message appears: *Warning: deleting a partition is irreversible.*
4. Click **OK** to continue.

If you delete the Active partition, all of its incidents are removed, but the Active partition itself cannot be deleted. The Status line for the deleted partitions indicates their deletion.

Archive threshold

You get warning messages when disk space is approaching the allocated threshold and when that threshold is exceeded. If you get the preliminary warning, archive the oldest records until at least 15% of allowed disk space is free. As a safeguard, Data Security automatically creates a “private” archive when disk space is exceeded. Should it be necessary, please contact Websense Technical Support to retrieve the archive.

14 Managing System Modules

Related topics:

- *Adding modules*, page 245
- *Configuring modules*, page 246
- *Balancing the load*, page 278

The System Modules screen lets you configure all the components in the Data Security network and distribute the load between them evenly.

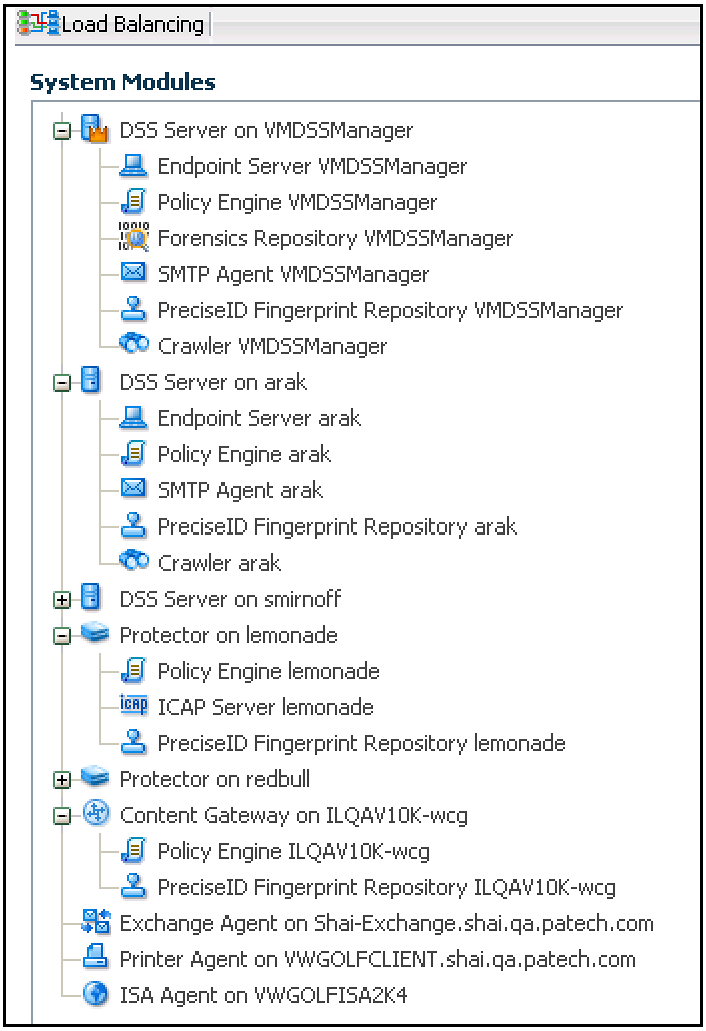
To access this screen, select **Settings** > **Deployment** > **System Modules**.

If you are running Websense Web Security Gateway Anywhere, the only modules you'll see listed on this screen are the Data Security Management Server and supplemental Data Security server(s) if any.

Each of these is comprised of several components, such as the fingerprint repository, crawler, and policy engine.

If you're running a full Websense Data Security deployment, you'll also see the protector and its components, as well as any stand-alone agents that you have installed. The nodes that appear in the System Modules tree depend on the options you selected during installation.

Each module and component is represented by an icon.

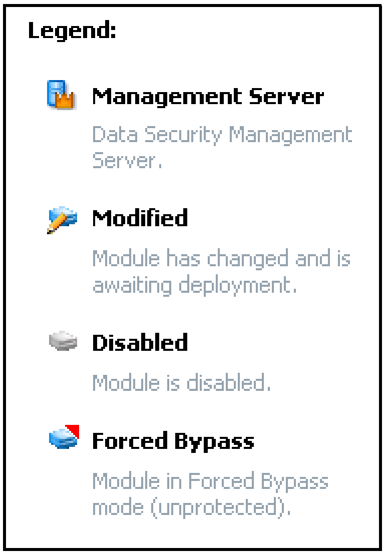


Load Balancing

System Modules

- DSS Server on VMDSSManager
  - Endpoint Server VMDSSManager
  - Policy Engine VMDSSManager
  - Forensics Repository VMDSSManager
  - SMTP Agent VMDSSManager
  - PreciseID Fingerprint Repository VMDSSManager
  - Crawler VMDSSManager
- DSS Server on arak
  - Endpoint Server arak
  - Policy Engine arak
  - SMTP Agent arak
  - PreciseID Fingerprint Repository arak
  - Crawler arak
- DSS Server on smirnoff
- Protector on lemonade
  - Policy Engine lemonade
  - ICAP Server lemonade
  - PreciseID Fingerprint Repository lemonade
- Protector on redbull
- Content Gateway on ILQAV10K-wcg
  - Policy Engine ILQAV10K-wcg
  - PreciseID Fingerprint Repository ILQAV10K-wcg
- Exchange Agent on Shai-Exchange.shai.qa.patech.com
- Printer Agent on VWGOLFCLIENT.shai.qa.patech.com
- ISA Agent on VWGOLFISA2K4

As shown in the on-screen legend, the icons are grayed-out when a component is disabled and they appear with a red exclamation point when the component has not yet been registered. If changes have been made to a module but have not yet been deployed, the icon appears with a pencil next to it.



Legend:

Management Server

Data Security Management Server.

Modified

Module has changed and is awaiting deployment.

Disabled

Module is disabled.

Forced Bypass

Module in Forced Bypass mode (unprotected).

If you have more than one Data Security server, there is a **Load Balancing** button on the toolbar. This button allows you to balance the load between your policy engines to optimize performance. See *Balancing the load*, page 278 for details.

Adding modules

To add a new module, go to the machine where you want to install it and run the Data Security installation wizard. (See the *Data Security Deployment Guide* for instructions.)

When you install the module, you are asked to provide the FQDN or the IP address of the Data Security Management Server and the credentials for a Data Security administrator with system modules permissions. When you do, the module is automatically registered with the management server.

If you accept the default configuration, click the **Deploy** button to complete the process. If you want to customize the configurations, go into the System Modules screen and click the module to edit. Follow the instructions in the next section.

Only a management user with system modules permissions can install new network elements. (See *Adding a new access role*, page 234 for information on system modules permissions.

Please note that if you install 2 stand-alone agents on the same machine (SMTP and printer, for example), Data Security registers them twice (independently) and they appear in the system-modules tree as 2 separate computers.

In addition, if the IP address or host name (FQDN) of a module should change after you've registered it, you must re-register the module to notify the Data Security Management Server of the change.

If you change both the IP address *and* the host name of a module, you must re-register it twice, once after each change. If you re-register once after both changes, the Data Security Management Server thinks it's a brand new module and does not retain the module's configuration information (minimum/maximum transaction size, monitoring mode, etc.).

Configuring modules

Related topics:

- *Adding modules*, page 245

If you have Websense Web Security Gateway Anywhere, you may never need to configure modules. The Data Security servers are given a default configuration when they're installed that usually suffices.

If you're running a full Websense Data Security deployment, in most cases, the only module that you *must* configure after installation is the protector. This is covered in Chapter 3: Initial Setup in the section *Configuring the protector*. However, if you're deploying an Exchange or ISA agent, these may need to be configured as well.

Either way, you are welcome to customize your configuration settings any time to meet your needs.

To configure a Data Security module:

1. Select **Settings** > **Deployment** > **System Modules**.
2. Click the module of interest.
3. Complete the fields as shown in the sections below:

> ✓ **Note**
> If you have Websense Web Security Gateway Anywhere, not all of these options apply to you.

- *Configuring the management server*
- *Configuring a supplemental Data Security Server*
- *Configuring the SMTP agent*
- *Configuring the PreciseID fingerprint repository*
- *Configuring the endpoint server*
- *Configuring the crawler*
- *Configuring the forensics repository*
- *Configuring the policy engine*
- *Configuring the protector*

- *Configuring ICAP*
- *Configuring the Content Gateway agent*
- *Configuring the ISA agent*
- *Configuring the printer agent*
- *Configuring the Exchange agent*
- *Configuring protector services*

Configuring the management server

The Data Security Management Server is the heart of the Websense Data Security system. It provides the core information loss technology, analyzing traffic on your network and applying policies to incidents. All other modules register and synchronize with the management server. You can change the FQDN of the management server, but you will have to run the Modify action on the installer, and re-register all agents, if for example, you want to join a manager into a domain. You cannot delete the management server, but you can change the name and description if desired. To do so, click the management server on the System Modules screen. This is the module with the crown .

Field	Description
Type	The type of module (uneditable).
Name	Enter a new name for the Data Security Management Server if desired. Not to exceed 128 characters.
Description	Enter a description for the management server, not to exceed 4000 characters.
FQDN	The fully qualified domain name given to the module when it was installed. (uneditable)

Configuring a supplemental Data Security Server

Field	Description
Type	The type of module (uneditable).
Name	Enter a new name for the Data Security Server if desired. Not to exceed 128 characters.
Description	Enter a description for the supplemental server, not to exceed 4000 characters.
FQDN	The fully qualified domain name given to the module when it was installed. (uneditable)

Note that you can delete a supplemental Data Security server, but you cannot delete the management server.

Configuring the SMTP agent

Related topics:

- *General tab*, page 248
- *SMTP Filter tab*, page 249
- *Encryption & bypass tab*, page 249
- *Advanced tab*, page 250

You can install the SMTP agent on the Data Security Management Server or you can install the stand-alone agent on an SMTP server. To configure the SMTP agent, select it on the System Modules screen and the Edit SMTP Agent window appears.

There are 4 tabs in this window:

- *General tab*
- *SMTP Filter tab*
- *Encryption & bypass tab*
- *Advanced tab*

General tab

Field	Description
Type	The type of module (uneditable).
Enabled	Select this box to enable the module for use in your environment. Deselect it to disable it. (Agents are enabled by default.)
Name	The name of the module (uneditable).
Description	Enter a description of the module.
FQDN	The fully qualified domain name given to the module when it was installed. (uneditable)
Mode	Select the mode in which you want to deploy the module: • **Monitoring** - Select Monitoring if you want to monitor SMTP traffic but not block it. • **Blocking** - Select Blocking if you want to block SMTP actions that breach policy.
When an unspecified error occurs	This option is only available for blocking mode. Select what action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed—for example, if a transaction timeout threshold has been exceeded: • **Permit traffic** - Allow SMTP traffic to continue unprotected. • **Block traffic** - Stop all SMTP traffic until the problem is resolved.

SMTP Filter tab

Field	Description
Enable inspection on the following internal email domains	Select this check box to enable inspection on specified domains, then add the domains to monitor.
Domains to monitor	Enter the domain name to monitor in the field provided then click Add to add it to the list. Continue until you've added all the domains of interest.

Encryption & bypass tab

Field	Description
Enable redirection gateway	If you want encrypted or flagged email to bypass content analysis, select this box, then enter the redirection gateway IP address and port number. This lets Data Security know where to send traffic that is supposed to be encrypted or is set to bypass analysis.
Encryption	
Verify that at least one of the following conditions is met	Select this box if you want Data Security to verify that a certain condition is met before sending email to the redirection gateway. Specify the condition by selecting one of the boxes below.
Subject contains encryption flag	One way to inform Data Security that email is to be sent to the encryption gateway is by inserting a specific string, or flag, in the Subject field of the message. In the event that a policy specifies that certain content should be encrypted, this flag will automatically be added to the subject field. Enter the flag to use here.
X-header field name	Email messages contain metadata referred to as x-headers. If you click **Encrypt** in Outlook or similar applications, an x-header is added to the message. In this field, specify the x-header field name that should signal Data Security to send messages to the encryption gateway.
Bypass	
Verify that at least one of the following conditions is met	Select this box if you want Data Security to verify that a certain condition is met before sending email to the redirection gateway. Specify the condition by selecting one of the boxes below.

Field	Description
Subject contains Bypass Flag	Enter the flag to add to the email Subject field when Bypass is desired.
X-Header Field Name	In this field, specify the x-header field name that should signal Data Security to send messages to the redirection gateway.

Advanced tab

Field	Description
Add the following footer to all email messages monitored by Data Security	Edit the default footer that is included in all email messages sent by Data Security.

Configuring the PreciseID fingerprint repository

In Data Security, secondary fingerprint repositories are stored on protectors, Content Gateways, and Data Security Servers while the primary repository is stored on the Data Security Management Server. This page depends on whether you are editing a primary or secondary/tertiary fingerprint repository.

- *Primary repository*
- *Secondary repository*

Primary repository

Field	Description
Type	The type of agent (uneditable).
Name	The name of the module (uneditable).
Description	Enter a description of the module, not to exceed 4000 characters.
Tuning Performance	
Maximum disk space	Select the maximum disk space that should be allowed for the PreciseID fingerprint repository, in megabytes.
Maximum cache size	Select the maximum amount of memory that the PreciseID fingerprint repository should use to cache fingerprints, in megabytes.
Mainly for detection	Select this option if you'd like the majority of memory that you allocated for the fingerprint repository to be used for detecting fingerprinted data so you can optimize this process.
Mainly for insertion	Select this option if you'd like the majority of memory that you allocated to be used for inserting fingerprinted data in the fingerprint repository so you can optimize this process. Select this option when you are running large fingerprinting tasks during off hours.

Secondary repository

Field	Description
Type	The type of agent (uneditable).
Name	The name of the module, not to exceed 128 characters.
Description	Enter a description of the module, not to exceed 4000 characters.

Field	Description
Detect fingerprints from:	Select a radio button to indicate where fingerprint detection should be performed: - **The repository installed on** - Select this option if you want detection performed on a remote repository, then select the server where the repository resides. Normally, you would select the primary repository on the Data Security Management Server, but you can select any repository. Websense recommends you choose one on the same LAN as this one. If you select the primary repository, you never have to perform synchronization. The primary repository is always up to date with the most recent fingerprints. - **This local repository** - Select this option if you want detection performed locally. If you choose this option, performance tuning options are enabled. Synchronization occurs only when this repository does not have the most up-to-date fingerprints. If you select this option, indicate how Data Security should use the fingerprinting memory, and schedule the synchronization based on your networking requirements.
Tuning Performance	
Maximum cache size	Select the maximum amount of memory that should be allocated for the PreciseID fingerprint repository, in megabytes.
Synchronize data with the primary repository	Secondary repositories must be synchronized with the primary periodically. You can choose 1 of 2 methods: - **Every n hours** - The secondary fingerprint repository is synchronized with the primary according to this interval. Using this setting, you can assure that fingerprinted data is protected by this device after no more than the specified number of hours. - **Every day at HH:MM** - The secondary fingerprint repository is synchronized with the primary every 24 hours at the specified time. Websense recommends you select a time during low traffic volume.

Configuring the endpoint server

Related topics:

- *Adding an endpoint profile*, page 282
- *Configuring endpoint settings*, page 290

The endpoint server is the server component of Websense Data Endpoint. Endpoint servers receive incidents from, and send configuration settings to, endpoint clients.To configure the endpoint server, select it on the System Modules screen and complete the fields as follows

Field	Description
Type	The type of module (uneditable).
Enabled	Select this box to enable the module for use in your environment. Deselect it to disable it.
Name	The name of the module, not to exceed 128 characters.
Description	Enter a description of the module, not to exceed 4000 characters.
FQDN	The fully qualified domain name given to the module when it was installed. (uneditable)

Configuring the crawler

Related topics:

- *PreciseID Fingerprinting - files & directories*, page 84
- *PreciseID Fingerprinting - database records*, page 89
- *Scheduling network discovery tasks*, page 138
- *Scheduling endpoint discovery tasks*, page 155

The crawler is the agent that performs fingerprint and discovery scans. You can have multiple crawlers in your Data Security system. To configure one, select it on the System Modules screen and complete the fields as follows.

Field	Description
Type	The type of module (uneditable).
Name	The name of the module (uneditable)
Description	Enter a description of the module, not to exceed 4000 characters.
FQDN	The fully qualified domain name given to the module when it was installed. (uneditable)

Configuring the forensics repository

Related topics:

- *Setting preferences for data usage incidents*, page 211

The forensics repository contains complete information about your original transactions. In SMTP, for instance, it stores the original email message that was sent.

For other channels, the system translates transactions into EML.

To configure the forensics repository, select it on the System Modules screen and complete the fields as follows:

Field	Description
Type	The type of module (uneditable).
Name	The name of the module (uneditable).
Description	Enter a description of the module, not to exceed 4000 characters.
FQDN	The fully qualified domain name given to the module when it was installed. (uneditable)
Forensics path	Enter the complete path where you want the forensics repository to be stored.
Log on as	Select how Data Security should log onto the server specified: ◆ **Local account** - Select this option to log on as a local user. (Primarily used when the path is local.) ◆ **This account** - Select this option to log on with specific user credentials, then enter the user name and password to use. Domain is optional.
Maximum disk space	Select the maximum disk space that should be allowed for the forensics repository, in megabytes (10,000 MB minimum) When the maximum is reached, the oldest records are moved to the archive folder to free space.

Configuring the policy engine

The policy engine is responsible for parsing your data and using analytics to compare it to the rules in your policies. You can have multiple policy engines in your Data Security system to manage high transaction volumes.

- There is always a policy engine on the Data Security Management Server and protector.
- If you have a supplemental Data Security server, there is one there as well.
- If you are combining Websense Web and Data Security solutions, there is a policy engine on the Websense Content Gateway.

To configure one of the policy engines, select it on the System Modules screen and the Edit Policy Engine window appears.

Tip

Balance the load between your policy engines by clicking the Load Balancing button on the System Modules toolbar. Refer to *Balancing the load*, page 278 for more information.

Field	Description
Type	The type of module (uneditable).
Enabled	Select this box to enable the module for use in your environment. Deselect it to disable it.
Name	The name of the module (uneditable).
Description	Enter a description of the module, not to exceed 4000 characters.
FQDN	The fully qualified domain name given to the module when it was installed. (uneditable)

Configuring the protector

Related topics:

- *General tab*, page 256
- *Networking tab*, page 256
- *Local Networks tab*, page 259
- *Services tab*, page 260

Once registration is established between the protector and the Data Security Management Server, clicking on the protector lets you set up advanced parameters.

To configure the protector, select it on the System Modules screen and the Edit Protector window appears.

There are 4 tabs in the Edit Protector window:

- *General tab*
- *Networking tab*
- *Local Networks tab*

- *Services tab*

Tip

You can also use the protector CLI to configure the protector. See the Deployment Guide, Appendix A for details on the CLI.

General tab

The General tab enables you to modify the basic settings of the protector.

Field	Description
Name	The name of the protector
Enabled	Select this box to enable this protector for use in your environment. Deselect it to disable it.
Description	Enter a description of the protector.
Host name	The host name of the machine hosting the protector
IP address	The IP address of the machine hosting the protector
Managed by	The name of the Data Security Server that is currently managing this protector.

Following are the 3 most common inline protector topologies:

- HTTP as active bridge
- HTTP and SMTP in monitoring bridge mode
- SMTP in MTA mode

If you are using one of these, make sure that the protector is enabled and that **Collect protector statistics** is selected.

Networking tab

The Networking tab lets you set protector networking properties. Please note that if your protector is in Inline mode, users lose an Internet connection for approximately 5 seconds when you deploy changes to network settings,

Field	Description
Default gateway	In the Default Gateway field, type the default gateway server router’s IP address, in the format X.X.X.X. The default gateway’s IP address should be from the same subnet of eth0’s network.
Interface	Select an interface to which packets for this route will be sent.
DNS servers	To add a DNS server, type in the DNS Server IP address and click Add. The DNS Server is added to the list.

Field	Description
DNS suffixes	Type the DNS suffix and click the Add button (optional). The domain suffix is used by the resolver while trying to resolve non FQDN names.
Connection mode	Select one of the following connection modes from the pull-down list: ◆ **Inline (Bridge)** - In Inline (Bridge), the protector is placed directly on the path between the corporate LAN and the Internet and can monitor and/or block traffic. ◆ **SPAN/Mirror Port** - In SPAN/Mirror Port, the protector can only monitor the traffic and cannot interfere with it. In this mode the protector is placed off a switch/TAP port which will relay all traffic traversing the network to the protector for analysis.
Network Interfaces	There are 4 types of network interfaces: Management, Bridge, Monitoring, and Network. To configure the protector's interfaces, click on the name of the interface. The options that appear depend on whether this is an inline or SPAN connection. See the relevant section below: ◆ *Interface configuration in Inline (Bridge) mode* ◆ *Interface configuration in SPAN/Mirror Port mode*
Enable VLAN support	If the monitored traffic contains VLAN tagging, select the **Enable VLAN Support** check box to monitor these networks.

If you are using HTTP in active bridge mode or monitoring bridge mode, make the following selections on this tab:

- Set **Default Gateway** to the outbound gateway.
- Select the **Connection mode** (Inline/Bridge).
- Edit the network interface br0 as follows:
  - Select **Enable bypass mode** to allow traffic in case of Data Security Server software/hardware failure.
  - Select **Force bypass** to enable an immediate bypass of traffic from the protector. The action is delayed (30 seconds) in order to allow the protector session to terminate successfully (switching off, though, takes place immediately).

Interface configuration in Inline (Bridge) mode

By default most appliances are equipped with 2 network cards on the motherboard. When working in inline mode, it is necessary to add 2 additional interfaces to be used as the bridge interfaces.

When using the protector in inline bridge mode, it is imperative that communication traffic continues. We've designed the system so that if there is a failure of any kind—from an application glitch to a power failure—the bridge will be short-circuited and the traffic will still go through. However, use of a special NIC further ensures that unforeseen difficulties not recognized by our software watchdog won't interrupt traffic flow.

When you use the certified Bypass Server Adapter NIC, any software failure results in the NIC moving into short-circuit mode. That disabling of the NIC hardware still allows your traffic to flow without interruption. If the special NIC is not installed, a software failure results in stalled traffic, so there is an advantage in employing the special NIC.

Once Inline (Bridge) is selected, eth2 and eth3 are replaced by br0 in the Network Interfaces table. Note that if eth2 and eth3 do not exist in the protector's hardware, the option of working in Inline (Bridge) is not available. Set eth0 as the Management Port.

In the Interface configuration screen, complete the fields as shown in the table below. The br0 interface uses 2 of the protector's interfaces and bridges them. The system needs more than 2 interfaces for bridging to be supported.

If the router and the firewall are on the same VLAN, the Bridge IP address and subnet mask must be valid on this VLAN.

In Inline (Bridge), no other protector interfaces can be set as monitoring interfaces. When a bridge is defined, it uses eth2 and eth3 interfaces.

✓ **Note**

In Inline (Bridge) mode, the IP address of the management interface cannot be modified. The protector selects a management interface automatically during CLI configuration, ordinarily, this interface is eth0.

Property	Description
Bridge name	The name of the inline bridge (uneditable)
Link Speed	Set the Link Speed to either: **10Mb/s, 100 Mb/s, 1000Mb/s, Automatic**.
Duplex Mode	Set Duplex Mode to either **Half**, **Full** or **Automatic**.
Enable bypass mode	Bypass can be used in the event that the Bypass Server Adapter NIC was ordered with the protector. It enables transparent failover in the event of protector failure. When Bypass is selected, if the protector malfunctions or is powered off, traffic transparently passes through the protector to the external network and data continues to flow. Deselect this option if you want all traffic to be stopped until the protector is up again.
Force bypass	Initiates an immediate bypass of traffic from the protector. The action is delayed (30 seconds) in order to allow the protector session to terminate successfully (switching off, though, takes place immediately).

While in Inline (Bridge) mode, interfaces that are not part of the bridge cannot work as Monitoring interfaces. If the interface Operation Mode is set to Monitoring, the interface Status is forced to Down.

Interface configuration in SPAN/Mirror Port mode

To configure the protector's interfaces in SPAN/Mirror Port mode, complete the fields as shown in the table below. All other interfaces can be set as Monitoring interfaces.

* Note that the Management Port can also be used for ICAP - specifying an additional port is optional. The additional port can also be set when configured as MTA.

Field	Description
Interface name	The name of the interface
Status	Set the status of the Interface to Up or Down. The status is learned from the protector but can be forced manually by selecting the Up/ Down radio button as necessary.
Mode	Set the interface's Operation Mode to either Network or Monitoring.
Interface IP address	Enter the interface's IP address. If Monitoring mode is selected this is not displayed; there is no need for an IP address for eth1 in Monitoring mode.
Subnet mask	Enter the subnet mask for the interface.
Link speed	Set the link speed to either: **10Mb/s, 100 Mb/s, 1000Mb/s, Automatic**.
Duplex mode	Set duplex mode to either **Half**, **Full** or **Automatic**.

Local Networks tab

To set which traffic the protector will monitor, select the **Local Networks** tab. Select either:

- **Include all networks** connected to the protector network.

> ✓ **Note**
>
> If you choose **All Networks**, traffic is monitored in all directions - incoming as well as outgoing and any configured direction is ignored. Choosing **All Networks** may drastically increase the load on the system and the system may collect unnecessary traffic.

- **Include specific networks**. To add specific networks click the **Add** button.

Insert the Network Address and Subnet Mask, for example: 10.10.1.0 and 255.255.255.0.

Added networks appear in the table and can be removed or edited using the appropriate buttons.

By default, Include specific networks is selected, and the common lists of non-routable IP addresses (per RFC1918) are included by default: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. If using Specific Networks, make sure that all the organization's internal IP addresses are included in this list. This list enables the protector to learn which connections are incoming and which are outgoing. These networks are referred as my networks while considering incoming/outgoing/internal directives for the different channels.

If you are using one of the 3 most common inline protector topologies:

- HTTP as active bridge
- HTTP and SMTP in monitoring bridge mode
- SMTP in MTA mode

be sure to select **Include specific networks.** Add all the internal networks for all sites. The mail servers and mail relays should be considered part of the internal network; this list is used to identify the direction of the traffic.

Click the **OK** button to apply the settings.

Services tab

To set protector services properties, click the **Services** tab in the Edit Protector dialog box.

Listed are all the services that have been configured for the protector, whether they are enabled or disabled, their ports, a direction (incoming, outgoing, or internal), and a description.

Click any service name to modify its settings.

Click **New** to add a new service.

Each protector can have only one service per port. One service can be removed for port 80 and a different one can be added but no 2 services can run on the same port.

Channels that can block traffic in Bridge/Inline mode require additional settings.

When working in inline mode, setting the direction is very important—in SMTP and HTTP, only outbound traffic should be analyzed. A misconfigured direction setting can cause the protector to send large amounts of data for analysis, degrading system performance. In addition, internal SMTP traffic (for example, between Exchange Servers) may be blocked by the system due to protocol incompatibility.

See *Configuring protector services*, page 267 for details on configuring protector services. There are 6 possible channels to configure.

- *Configuring SMTP*
- *Configuring HTTP*
- *Configuring FTP*
- *Configuring chat*
- *Configuring plain text*

Configuring ICAP

The protector supports Internet Content Adaptation Protocol (ICAP) and can be an integration point for third-party solutions that support ICAP, such as some Web proxies. To configure an ICAP server on the protector, select the ICAP server on the System Modules screen and the Edit ICAP window appears.

There are 3 tabs in the Edit ICAP window:

- *General tab*
- *HTTP tab*
- *FTP tab*

General tab

Field	Description
Type	The type of module (uneditable).
Enabled	Select this box to enable the module for use in your environment. Deselect it to disable it.
Name	The name of the module (uneditable).
Description	Enter a description of the module.
Ports	Enter the ports used by this ICAP server. These are the ports over which Data Security should monitor ICAP transactions. Separate multiple values with commas. Example: 1333,1334
Allow connection to this ICAP Server from the following IP addresses:	Select whether you want this ICAP server to allow connections from all IP addresses or just selected IP addresses. If you choose Selected, enter the IP address to allow then click Add. Repeat this process until you've added all the IP addresses you want to allow.

HTTP tab

Field	Description
Mode	Select the mode in which you want to deploy the module: • **Monitoring** - Select Monitoring if you want to monitor HTTP traffic but not block it. • **Blocking** - Select Blocking if you want to block HTTP actions that breach policy.
When an unspecified error occurs	Select what action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed: • **Permit traffic** - Allow HTTP traffic to continue unprotected. • **Block traffic** - Stop all HTTP traffic until the problem is resolved.

Field	Description
Minimum transaction size	Select the smallest size transaction that you want Data Security to monitor, in bytes.
Default violation message	Click the link to see the error message that is displayed on the user's browser when a URL is blocked due to a policy violation.
Default unspecified error message	Click the link to see the error message that is displayed when a URL is blocked due to an unspecified error.

FTP tab

Field	Description
Mode	Select the mode in which you want to deploy the module: • **Monitoring** - Select Monitoring if you want to monitor FTP traffic but not block it. • **Blocking** - Select Blocking if you want to block FTP actions that breach policy.
When an unspecified error occurs	Select what action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed: • **Permit traffic** - Allow FTP traffic to continue unprotected. • **Block traffic** - Stop all FTP traffic until the problem is resolved.
Minimum transaction size	Select the smallest size transaction that you want Data Security to monitor, in bytes.

Configuring the Content Gateway module

The Websense Content Gateway is a Web proxy that is an integral part of Websense Web Security Gateway and Web Security Gateway Anywhere solutions. If you have Websense Web Security or Websense Web Filter and you want to combine it with Websense Data Security solutions, you must have the Websense Content Gateway.

When you register the Websense Content Gateway with the Data Security Management Server, the Content Gateway module appears in the System Modules screen.

To configure the Content Gateway module, select it on the System Modules screen and the Edit Websense Content Gateway window appears.

There are 3 tabs in the Edit Websense Content Gateway window:

- *General tab*
- *HTTP tab*
- *FTP tab*

General tab

Field	Description
Type	The type of module (uneditable).
Enabled	Select this box to enable the module for use in your environment. Deselect it to disable it.
Name	The name of the module (uneditable).
Description	Enter a description of the module.
FQDN	The fully qualified domain name given to the module when it was installed. (uneditable)

HTTP tab

Field	Description
Mode	Select the mode in which you want to deploy the module: ◆ **Monitoring** - Select Monitoring if you want to monitor HTTP traffic through the Websense Content Gateway but not block it. ◆ **Blocking** - Select Blocking if you want to block HTTP actions that breach policy.
When an unspecified error occurs	Select what action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed: ◆ **Permit traffic** - Allow HTTP traffic routed through the Websense Content Gateway to continue unprotected. ◆ **Block traffic** - Stop all HTTP traffic through the gateway until the problem is resolved.
Minimum transaction size	Select the smallest size transaction that you want Data Security to monitor, in bytes.
Display default violation message	Select this radio button to display a default violation message in the user's browser whenever a URL violation is detected. Click the link to view the message.
Display custom message	Select this button to use a custom message, then browse to the message to use. (This file must be fewer than 2800 characters.)

FTP tab

Field	Description
Mode	Select the mode in which you want to deploy the module: - **Monitoring** - Select Monitoring if you want to monitor FTP traffic through the Websense Content Gateway but not block it. - **Blocking** - Select Blocking if you want to block FTP actions that breach policy.
When an unspecified error occurs	Select what action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed: - **Permit traffic** - Allow FTP traffic routed through the Websense Content Gateway to continue unprotected. - **Block traffic** - Stop all FTP traffic through the gateway until the problem is resolved.
Minimum transaction size	Select the smallest size transaction that you want Data Security to monitor, in bytes.

Configuring the ISA agent

The ISA agent is installed on your Microsoft ISA Server. To configure the ISA agent, select it on the System Modules screen and the Edit ISA Agent window appears.

There are 2 tabs in the Edit ISA Agent window:

- *General tab*
- *Advanced tab*

General tab

Field	Description
Type	The type of module (uneditable).
Enabled	Select this box to enable the module for use in your environment. Deselect it to disable it.
Name	The name of the module (uneditable).
Description	Enter a description of the module, not to exceed 4000 characters.
FQDN	The fully qualified domain name given to the module when it was installed. (uneditable)

Field	Description
Operation mode	Select the mode in which you want to deploy the module: - **Monitoring** - Select Monitoring if you want to monitor traffic through the ISA server but not block it. - **Blocking** - Select Blocking if you want to block actions that breach policy.
When an unspecified error occurs	Select what action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed: - **Permit traffic** - Allow traffic routed through the ISA server to continue unprotected. - **Block traffic** - Stop all traffic through the ISA server until the problem is resolved.

Advanced tab

Field	Description
Display default message	Select this button to display a default message in the user's browser when a URL is blocked due to a policy violation. Click the link to view the message.
Display custom message	Select this button to use a custom message, then browse to the message to use. (This file must be fewer than 2800 characters.)

Configuring the printer agent

The printer agent is installed on your print server. To configure the printer agent, select it on the System Modules screen and the Edit Printer Agent window appears. Complete the fields as follows:

Field	Description
Type	The type of module (uneditable).
Enabled	Select this box to enable the module for use in your environment. Deselect it to disable it.
Name	The name of the module (uneditable).
Description	Enter a description of the module, not to exceed 4000 characters.
FQDN	The fully qualified domain name given to the module when it was installed. (uneditable)

Field	Description
Mode	Select the mode in which you want to deploy the module: • **Monitoring** - Select Monitoring if you want to monitor traffic through the print server but not block it. • **Blocking** - Select Blocking if you want to block actions that breach policy.
When an unspecified error occurs	Select what action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed: • **Permit traffic** - Allow traffic routed through the print server to continue unprotected. • **Block traffic** - Stop all traffic through the print server until the problem is resolved.

Configuring the Exchange agent

The Exchange agent is installed on your Microsoft Exchange Server. To configure the Exchange agent, select it on the System Modules screen and the Edit Exchange Agent window appears.

There are 2 tabs in the Edit Exchange Agent window:

- *General tab*
- *Exchange Filter tab*

General tab

Field	Description
Type	The type of module (uneditable).
Enabled	Select this box to enable the module for use in your environment. Deselect it to disable it.
Name	The name of the module (uneditable).
Description	Enter a description of the module, not to exceed 4000 characters.
FQDN	The fully qualified domain name given to the module when it was installed. (uneditable)
Mode	Select the mode in which you want to deploy the module: • **Monitoring** - Select Monitoring if you want to monitor traffic through the print server but not block it. • **Blocking** - Select Blocking if you want to block actions that breach policy.
When an unspecified error occurs	Select what action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed: • **Permit traffic** - Allow traffic to the Exchange server continue unprotected. • **Block traffic** - Stop all traffic until the problem is resolved.

Exchange Filter tab

Field	Description
Enable filter	Select this check box to enable the Exchange filter. This allows the filter to monitor internal email domains. Enter the internal email domain to monitor then click **Add**. Repeat until you added all the domains you want Data Security to monitor. Do not leave this empty (all email will be analyzed).

Configuring protector services

Related topics:

- *Configuring the policy engine*, page 254
- *Configuring SMTP*, page 267
- *Configuring HTTP*, page 272
- *Configuring FTP*, page 274
- *Configuring chat*, page 275
- *Configuring chat*, page 275
- *Configuring plain text*, page 277

There are several services that the protector can monitor. To configure the services, go to System Modules, select the protector, select the **Services** tab, and click the service you want to configure:

- SMTP
- HTTP
- FTP
- Plain text
- Chat
- telnet

Configuring SMTP

There can be 3 or 5 tabs in the Edit SMTP Service window, dependent on the mode you select on the General tab. If you select a monitoring mode, the following 3 tabs appear:

- *General tab*

- *Traffic Filter tab*
- *SMTP Filter tab*

If you select Mail Transfer Agent (MTA) mode, 2 additional tabs appear:

- *Mail Transfer Agent (MTA) tab*
- *Encryption & Bypass tab*

General tab

Field	Description
Type	The type of module (uneditable).
Enabled	Select this box to enable the module for use in your environment. Deselect it to disable it.
Name	The name of the module (uneditable).
Description	Enter a description of the module.
Ports	Enter the ports to monitor, separated with commas. Example: 1333,1334
Intelligent protocol discovery	Select this check box if you want Data Security to match data from unknown ports to this SMTP service. If enabled, the protector tries to parse the transaction regardless of the port number. (Note that this has an effect on protector performance.)
Mode	If the protector is operating in inline mode, select which of the following modes to use: • **Monitoring bridge** - In monitoring bridge mode, Websense Data Security monitors and analyzes a copy of the traffic but does not enable policies to block transactions. • **Mail Transfer Agent** - Select this option to set the protector to MTA mode. You must configure your mail servers and clients to forward mail tot the protector. Note that when functioning as an MTA, it is important to make sure to limit the networks monitored by the protector in order to prevent the protector from becoming an open relay. If the protector is operating in SPAN mode, select which of the following modes to use: • **Monitoring passive** - In monitoring passive mode, Websense Data Security monitors and analyzes a copy of all traffic but does not enable policies to block transactions. • **Mail Transfer Agent** - Select this option to set the protector to MTA mode. You must configure your mail servers and clients to forward mail tot the protector. Note that when functioning as an MTA, it is important to make sure to limit the networks monitored by the protector in order to prevent the protector from becoming an open relay.

If you are using MTA mode, be sure to set the **Mode** to **MTA.**

If you are using monitoring bridge mode, set the **Mode** to **Monitoring Bridge.**

Traffic Filter tab

Field	Description
Transaction Size	
Minimum transaction size	Select the smallest size transaction that you want Data Security to monitor, in bytes.
Direction	
Incoming	Select **Incoming** if you want Data Security to monitor incoming SMTP traffic.
Outgoing	Select **Outgoing** if you want Data Security to monitor outgoing SMTP traffic.
Internal	Select **Internal** if you want Data Security to monitor internal SMTP traffic.
Source's Network	
Enable filter	Select this check box to enable the source's network filter. This tells Websense Data Security to watch for messages sent from specific networks and not analyze those messages. Enter the network IP address and subnet mask to not analyze then click **Add**. Repeat this process for each network address you want to skip.

If you are using HTTP in active bridge mode or monitoring mode, be sure to set the **Direction** mode as outgoing *only!*

SMTP Filter tab

Field	Description
Direction	
Enable filtering on the following internal email domains	Select this check box to enable the SMTP filter, then enter the internal email domains to monitor and click Add. Repeat this process for each internal email domain you want to monitor.
Domain	Enter the name of an internal email domain to monitor and click **Add**. Do this for each internal email domain that you want to monitor.
Incoming	Select **Incoming** if you want Data Security to monitor incoming SMTP traffic.
Outgoing	Select **Outgoing** if you want Data Security to monitor outgoing SMTP traffic.
Internal	Select **Internal** if you want Data Security to monitor internal SMTP traffic.

Field	Description
Source's Email Address	
Enable filter	Select this check box to enable the source's email address filter. This tells Data Security to watch for messages sent from specific email address and not analyze those messages. Enter the email address to not analyze then click Add. Repeat this process for each email address you want to skip.

Mail Transfer Agent (MTA) tab

This tab applies only to inline protector mode.

Field	Description
Operation Mode	
Monitoring	Select this mode if you want to monitor SMTP traffic only.
Blocking	Select this mode if you want to block SMTP traffic that breaches policy.
Permit traffic	Select this action if you want to allow all SMTP traffic through in the event an unspecified error occurs during data analysis, and traffic cannot be analyzed.
Block traffic	Select this option if you want to block all SMTP traffic in the event of an unknown error.
SMTP Settings	
SMTP HELO name	For SMTP traffic set to work as an MTA, it is necessary to set the HELO name. Enter the HELO name here; do not include spaces. This setting configures the name the protector uses to communicate with the next hop. This is the string that the MTA uses to identify itself when it connects with other servers.
Set next hop MTA	A next hop MTA (or Smart Host) can be set to define the mail server/gateway to which the protector should forward traffic after analysis.
Maximum message size	Sets the maximum size for email when the SMTP service is being run in the MTA mode. By default, this is set to 33 MB.
Network address	It is important that not all networks have permission to send email via the protector's SMTP service, otherwise the protector can be used as a mail relay. To avoid this, it is necessary to limit the networks that send email via the protector. Enter the network addresses that have permission here.
Subnet mask	Enter the subnet masks corresponding to the network addresses you entered above.
Email Settings	
Add the following footer	Enter the footer to add to email notifications to all email messages monitored by Data Security.
Send notifications	Select this option if you want to send notifications when there is a problem with email.

If you are using SMTP in MTA mode or HTTP in active bridge mode:

- Select the mode **Blocking**.
- Select the behavior desired when an **Unspecified error occurs** during analysis.
- Set the **SMTP HELO name.** If a mail relay is available then there may be no need to configure the HELO name if the mail relay provides this data.
- Set the **Next Hop** if required (e.g., company mail relay).

Encryption & Bypass tab

This tab applies only to inline protector mode.

Field	Description
Enable redirection gateway	If you want encrypted or flagged email to bypass content analysis, select this box, then enter the redirection gateway IP address and port number. This lets Data Security know where to send traffic that is supposed to be encrypted or is set to bypass analysis.
Encryption	
Verify that at least one of the following conditions is met	Select this box if you want Data Security to verify that a certain condition is met before sending email to the redirection gateway. Specify the condition by selecting one of the boxes below.
Subject contains encryption flag	One way to inform Data Security that email is to be sent to the encryption gateway is by inserting a specific string, or flag, in the Subject field of the message. In the event that a policy specifies that certain content should be encrypted, this flag will automatically be added to the subject field. Enter the flag to use here.
X-header field name	Email messages contain metadata referred to as x-headers. If you click **Encrypt** in Outlook or similar applications, an x-header is added to the message. In this field, specify the x-header field name that should signal Data Security to send messages to the encryption gateway.
Bypass	
Verify that at least one of the following conditions is met	Select this box if you want Data Security to verify that a certain condition is met before sending email to the redirection gateway. Specify the condition by selecting one of the boxes below.
Subject contains Bypass Flag	Enter the flag to add to the email Subject field when Bypass is desired.
X-Header Field Name	In this field, specify the x-header field name that should signal Data Security to send messages to the redirection gateway.

Configuring HTTP

To configure the protector's HTTP service, click **HTTP** on the **Services** tab. There are 4 tabs in the Edit HTTP Service window:

- *General tab*
- *Traffic Filter tab*
- *HTTP Filter tab*
- *Advanced tab*

General tab

Field	Description
Type	The type of module (uneditable).
Enabled	Select this box to enable the module for use in your environment. Deselect it to disable it.
Name	The name of the module (uneditable).
Description	Enter a description of the module.
Ports	Enter the ports to monitor, separated with commas. Example: 80,8080
Intelligent protocol discovery	Select this check box if you want Data Security to match data from unknown ports to this HTTP service. If enabled, the protector tries to parse the transaction regardless of the port number. (Note that this has an effect on protector performance.)
Mode	Select which of the following modes to use: • **Monitoring bridge** - In monitoring bridge mode, Websense Data Security monitors and analyzes a copy of all HTTP traffic but does not enable policies to block transactions. • **Active bridge** - In inline mode, Websense Data Security monitors and blocks traffic according to HTTP policies configured.

If you are using HTTP in active bridge mode, be sure to set the **Mode** to **Active Bridge.**

If you are using HTTP and SMTP in monitoring bridge mode, set the **Mode** to **Monitoring Bridge.**

Traffic Filter tab

Field	Description
Transaction Size	
Minimum transaction size	Select the smallest size transaction that you want Data Security to monitor, in bytes.
Direction	
Incoming	Select **Incoming** if you want Data Security to monitor incoming HTTP traffic.
Outgoing	Select **Outgoing** if you want Data Security to monitor outgoing HTTP traffic.
Internal	Select **Internal** if you want Data Security to monitor internal HTTP traffic.
Source's Network	
Enable filter	Select this check box to enable the source's network filter. This tells Data Security to watch for messages sent from specific networks and not analyze those messages. Enter the network IP address and subnet mask to not analyze then click Add. Repeat this process for each network address you want to skip.

If you are using HTTP and SMTP in active bridge mode or monitoring mode, be sure to set the **Direction** mode is outgoing *only!*

HTTP Filter tab

Field	Description
Exclude destination domains	Select this check box if you want to exclude certain domains from analysis, then enter the domains to exclude and click **Add**. To remove a domain from the exclusion list, select the domain and click **Remove**. When you are covering HTTP and SMTP in active bridge or monitoring mode, you may want to exclude domains here.

Advanced tab

Field	Description
Operation mode	Select the mode to use for HTTP traffic: - **Monitoring** - Select **Monitoring** if you want to monitor HTTP traffic only. - **Blocking** - Select **Blocking** if you want to block HTTP traffic that breaches policy.
Policy violation	
Display default message	Select this radio button to display a default message in the user's browser when a URL is blocked due to a policy violation. Click the **Default message** link to view the default message.
Redirect to URL	Select this option to redirect the page to an alternate URL when a URL is blocked due to a policy violation, then enter the URL to which to redirect traffic.
Unspecified error	
Permit traffic	Select this option if you want to permit HTTP traffic to continue unprotected when an unspecified error occurs during data analysis and traffic cannot be analyzed.
Block traffic	Select this action if you want to stop all HTTP traffic when an unspecified error occurs until the problem is resolved.
Display default message	Select this radio button to display a default message in the user's browser when a URL is blocked due to an unspecified error. Click the **Default message** link to view the default message.
Redirect to URL	Select this option to redirect the page to an alternate URL when a URL is blocked due to an unspecified error, then enter the URL to which to redirect traffic.

If you are using HTTP and SMTP in active bridge mode, select operation mode **Blocking**, and set the behavior desired when an unspecified error occurs during analysis.

Configuring FTP

To configure the protector's FTP service, click **FTP** on the **Services** tab. There are 2 tabs in the Edit FTP Service window:

- *General tab*
- *Traffic Filter tab*

General tab

Field	Description
Type	The type of module (uneditable).
Enabled	Select this box to enable the module for use in your environment. Deselect it to disable it.
Name	The name of the module (uneditable).
Description	Enter a description of the module.
Ports	Enter the ports to monitor, separated with commas. Example: 20,2121
Intelligent protocol discovery	Select this check box if you want Data Security to match data from unknown ports to this FTP service. If enabled, the protector tries to parse the transaction regardless of the port number. (Note that this has an effect on protector performance.)

Traffic Filter tab

Field	Description
Transaction Size	
Minimum transaction size	Select the smallest size transaction that you want Data Security to monitor, in bytes.
Direction	
Incoming	Select **Incoming** if you want Data Security to monitor incoming FTP traffic.
Outgoing	Select **Outgoing** if you want Data Security to monitor outgoing FTP traffic.
Internal	Select **Internal** if you want Data Security to monitor internal FTP traffic.
Source’s Network	
Enable filter	Select this check box to enable the source’s network filter. This tells Data Security to watch for messages sent from specific networks and not analyze those messages. Enter the network IP address and subnet mask to not analyze then click Add. Repeat this process for each network address you want to skip.

Configuring chat

To configure the protector’s Chat service, click **Chat** on the **Services** tab. There are 3 tabs in the Edit Chat Service window:

- *General tab*
- *Traffic Filter tab*
- *Advanced tab*

General tab

Field	Description
Type	The type of module (uneditable).
Enabled	Select this box to enable the module for use in your environment. Deselect it to disable it.
Name	The name of the module (uneditable).
Description	Enter a description of the module.
Ports	Enter the ports to monitor, separated with commas. Example: 20,2121
Intelligent protocol discovery	Select this check box if you want Data Security to match data from unknown ports to this FTP service. If enabled, the protector tries to parse the transaction regardless of the port number. (Note that this has an effect on protector performance.)

Traffic Filter tab

Field	Description
Transaction Size	
Minimum transaction size	Select the smallest size transaction that you want Data Security to monitor, in bytes.
Direction	
Incoming	Select **Incoming** if you want Data Security to monitor incoming FTP traffic.
Outgoing	Select **Outgoing** if you want Data Security to monitor outgoing FTP traffic.
Internal	Select **Internal** if you want Data Security to monitor internal FTP traffic.
Source's Network	
Enable filter	Select this check box to enable the source's network filter. This tells Data Security to watch for messages sent from specific networks and not analyze those messages. Enter the network IP address and subnet mask to not analyze then click Add. Repeat this process for each network address you want to skip.

Advanced tab

Field	Description
Wait	Select the maximum amount of time to wait before forwarding content to the Data Security server, in milliseconds.

Configuring plain text

To configure the protector’s telnet service, click **plain text** on the **Services** tab. There are 3 tabs in the Edit Plain Text Service window:

- *General tab*
- *Traffic Filter tab*
- *Advanced tab*

General tab

Field	Description
Type	The type of module (uneditable).
Enabled	Select this box to enable the module for use in your environment. Deselect it to disable it.
Name	The name of the module (uneditable).
Description	Enter a description of the module.
Ports	Enter the ports to monitor, separated with commas. Example: 5222, 5333

Traffic Filter tab

Field	Description
Transaction Size	
Minimum transaction size	Select the smallest size transaction that you want Data Security to monitor, in bytes.
Direction	
Incoming	Select **Incoming** if you want Data Security to monitor incoming FTP traffic.
Outgoing	Select **Outgoing** if you want Data Security to monitor outgoing FTP traffic.
Internal	Select **Internal** if you want Data Security to monitor internal FTP traffic.

Field	Description
Source's Network	
Enable filter	Select this check box to enable the source's network filter. This tells Data Security to watch for messages sent from specific networks and not analyze those messages. Enter the network IP address and subnet mask to not analyze then click Add. Repeat this process for each network address you want to skip.

Advanced tab

Field	Description
Stop processing connection if...	Select this check box to stop processing the connection if the binary data that is detected reaches a certain size threshold.
Binary character threshold	Select the maximum size, in characters, of binary data to process. If the data detected exceeds this threshold, the connection is no longer processed.
Text delimiter	Select a text delimiter from the pull-down list: tab, space, semicolon, or other. If you choose other, enter the character in the box provided.
Buffer interval	Select the maximum amount of time to wait before forwarding content to the Data Security server, in milliseconds.

Balancing the load

Related topics:

- *Defining load balancing distribution*, page 279

You may have several policy engines in your Data Security system. There is one on each Data Security server; there is one on the protector; and if you have Websense Web Security Gateway, or Web Security Gateway Anywhere, there is one on the Websense Content Gateway as well.

Policy engines are responsible for analyzing the data flowing through your enterprise, comparing it to policies, and governing remediation action, if any.

At times, a policy engine can become overloaded. The System Health screen can help you assess the impact that traffic is having on performance. Select **Main** > **Status & Logs** > **System Health.** Expand the relevant protector and select the policy engine to view. You can see the number of transactions being analyzed and the latency of each policy engine. (See *Monitoring system health*, page 200 for details.)

To distribute the processing load between more evenly:

1. Select **Settings > Deployment > System Modules**.
2. Click **Load Balancing** on the toolbar.

The resulting screen names all the modules, lists all the services being analyzed, and the policy engine doing the work. Click the plus (+) signs to expand the tree and view all available information.

To change the configuration, placing the load on different policy engines, click one or more of the services.

Defining load balancing distribution

Double-click a service to configure which policy engine should analyze it.

Field	Description
Service	The name of the service (uneditable)
DSS Server Protector Crawler ICAP Server Content Gateway	The host responsible for the service (uneditable).
Analyzed by	Select **All available policy engines** if you want the service analyzed by all available policy engines. The policy engine on the protector is available for the protector only. Select **Selected policy engines** if you want the service analyzed by the indicated policy engine only. If you choose this option, select the policy engine or engines you want to do the work.
Apply these settings to all of this protector’s services	Select this check box if you want to apply these settings to all of t his protector’s services without having to configure each manually.

15 Configuring Endpoint Deployment

Deploying endpoint systems in your network is comprised of the following basic steps:

1. Installing the Data Security Management Server as described in the *Websense Data Security Deployment Guide*.
2. Building a package for the endpoint client and deploying it on users' computers (PC, laptops, etc.) as described in the deployment guide.
3. *Adding an endpoint profile* to TRITON - Data Security or using the default. A default profile is automatically installed with the client package. (**Settings** > **Deployment** > **Endpoint**.)
4. *Rearranging endpoint profiles*. (**Settings** > **Deployment** > **Endpoint**.)
5. *Configuring endpoints*' settings. (**Settings** > **Configuration** > **System** > **Endpoint**, or **Settings** > **Deployment** > **Endpoint**, **Settings** button.)
6. Creating endpoint resources. (**Main** > **Policy Management** > **Resources** > *Endpoint Devices* / *Endpoint Applications* / *Endpoint Application Groups*.)
7. Creating or modifying a rule for endpoint channels. (**Main** > **Policy Management** > **Data Usage / Data Discovery Policies**, Destination tab.) See *Selecting endpoint destination channels to monitor*.
8. Defining the type of endpoint machines to analyze, as well as the network location. (**Main** > **Policy Management** > **Data Usage / Data Discovery Policies**, *Rule Wizard - Source* tab.) Use the Network Location field to define the behavior of the endpoint on and off the network.
9. Deploying endpoint configuration settings. (**Deploy** button.)
10. Viewing the status of endpoint systems. (**Main** > **Status & Logs** > **Endpoint Status**.) See *Viewing endpoint status*.
11. Viewing incidents detected by endpoints, and taking a number of actions on them, including editing the incident details, changing the severity of the incident, or escalating the incident to a manager. (**Main** > **Incidents & Reports** > **Data Usage**.) See *Viewing the incident list*.

In special circumstances, you can also bypass an endpoint client—that is, stop monitoring or protecting it for a period of time. See *Bypassing endpoint clients*, page 293 for more information on this capability.

For information on what end users see on their machine, refer to *Using the endpoint client software*, page 293.

Endpoint profiles

Endpoint profiles are templates that set service permissions. A profile describes the required behavior of an endpoint client: how it connects to endpoint servers, which user interface options are available on the client, and how it uses encryption keys to protect the transfer of sensitive data. Each profile is deployed to selected endpoint clients.

Endpoint clients

The endpoint client is a piece of Websense software that gets installed on an endpoint machine. It monitors real-time traffic and applies customized security policies to applications and storage media as well as data at rest. The client application enables administrators to analyze content within a user's working environment and block or monitor policy breaches as defined by the endpoint profiles. Administrators can create policies that allow full visibility of content without restricting device usage.

When an endpoint client is installed on a computer, it attempts to connect to a Data Security server to retrieve its policies and endpoint profile(s). As soon as its settings are deployed, the endpoint client starts running according to its profile settings.

Endpoint servers

The endpoint server component is installed automatically on the Data Security Management Server and supplemental Data Security servers. Endpoint servers receive incidents from, and send configuration settings to, endpoint clients.

Adding an endpoint profile

Related topics:

- *Rearranging endpoint profiles*, page 288
- *Deploying endpoint profiles*, page 288
- *General tab*, page 283
- *Servers tab*, page 284
- *Properties tab*, page 285
- *Encryption tab*, page 286

A default endpoint profile is automatically installed on the endpoint client. To add or edit an endpoint profile:

1. Select **Settings** > **Deployment** > **Endpoint**.

2. To create a new profile, select **New**. (To edit an existing profile, click a profile name in the list.).

> **Note**
>
> Websense Data Security includes a default profile. This profile is automatically applied to all endpoints not assigned to a specific endpoint profile. You can edit parts of the default profile, but you cannot delete it.

3. Complete the **General**, **Servers**, **Properties**, and **Encryption** tabs as described in the following sections.
4. Click **OK** when finished.

General tab

To define general settings for an endpoint profile:

1. Select the **General** tab.
2. Enter a name and a description for the profile.
3. Check the **Enabled** box to enable the profile in the endpoint profile list. If this check box is not selected, the profile is not deployed to any endpoint hosts.
4. By default, the profile is applied to all endpoints. If you want to include or exclude specific endpoints in the profile, click **Edit**.
5. Select an endpoint category from the **Display** drop-down list. The **Available List** updates to show available endpoints in that category.

> **Note**
>
> If you choose Directory Entries from the **Display** list, the Available List changes to show your default Active Directory location and the endpoints within it. If you are using your Active Directory, the **Filter by** field changes to a **Find** field.

6. To filter the available endpoints, enter text in the **Filter by** field. Click the Apply filter icon to enable the filter. Clicking the Clear filter icon removes the current filter.

   You can use wildcards in your filter: a question mark (?) to represent a single character, and an asterisk (*) for multiple characters.

> **Note**
>
> If there are too many items to fit on the screen, you can browse the list using the Next, Previous, First, and Last buttons.

7. To include a specific endpoint in this endpoint profile:
    a. In the **Selected List**, select the Include tab.
    b. In the **Available List**, select the endpoint.

> **Note**
> You can use the **Shift** and/or **Ctrl** keys to select multiple endpoint hosts.

    c. Click > to move the endpoint into the **Selected List**.
8. Click **OK**.
9. To exclude a specific endpoint in this endpoint profile:
    a. In the **Selected List**, select the Exclude tab.
    b. In the **Available List**, select the endpoint.
    c. Click > to move the endpoint into the **Selected List**.
10. Click **OK**.

Servers tab

This tab lists the Websense Data Security endpoint servers installed in the system. Each Data Security server within an organization automatically incorporates an endpoint server.

Incidents are sent to servers defined as Primary. If this fails, incidents are sent to servers defined as Secondary. If a server is defined as N/A, it neither receives incidents nor sends configuration settings to endpoints.

> **Note**
> You cannot deploy an endpoint profile if there are no active endpoint servers.

You can also use this tab to define the connection protocol between the endpoints and the endpoint servers.

To define server settings:

1. Select the **Servers** tab.
2. For each server, select one of the following from the **Priority** drop-down list:
    - **Primary -** All data is sent to this server for logging, policy, and profile updates. If you have multiple primary servers, endpoints are divided between the servers.
    - **Secondary -** If sending data to primary servers fails, data is sent to secondary servers. If you have multiple secondary servers, endpoints are divided between the servers.
    - **N/A -** Analysis is done locally in the endpoint client. Servers with an N/A status do not receive or send any data.

3. Select a connection type from the drop-down list. The default type is HTTPS.
4. If you want to use a proxy server for the connection, check the box and enter the proxy's IP address and port number.

> **Note**
>
> If you are using multiple Data Security servers, they are load-balanced: endpoint clients send and receive data to and from all available servers in their list.

Properties tab

Use the Properties tab to specify options for the following:

- **User interface options for interactive mode**. This means that a user interface is available on the endpoint to be displayed to its local user.
- **Endpoint message template**. Message templates are used for messages sent to the endpoint client, such as status details and alerts. The templates are XML files, and are available in the endpoint profile in multiple languages. The default template is the currently-defined template on the endpoint server.

  The templates are stored in the \custom\endpoint\msgFiles where Websense Data Security is installed.

- **Content policy settings**. This enables you to override settings on policies that are content-based.

To define properties settings:

1. Select the **Properties** tab.
2. Under Interactive Mode Options, do the following:
   a. Check the **Remote bypass** box to allow the endpoint user to disable the endpoint client. This action requires a bypass code from the administrator. (See *Bypassing endpoint clients*, page 293 for additional information.)
   b. Check the **Content scan alerts** box to alert the endpoint user when content scanning is in progress. A popup caption appears on the endpoint's screen.
3. To change the default endpoint message template, check the **Set message template to** box and select a new message template from the drop-down list.
4. Check **Disable blocking capabilities when policy violations are detected** to disable blocking on the endpoint if there is a content-related policy violation. Even if a policy is specifically set up to block content, the endpoint client overrides this setting and allows traffic. You might want to do this if a policy is preventing a user from doing his job: you can override the block for that specific endpoint.

Encryption tab

Related topics:

- *Backing up encryption keys*, page 289
- *Restoring encryption keys*, page 289

The Encryption feature allows legitimate users to transfer confidential information to removable media (such as an external hard drive or a CD/DVD) by encrypting the data before transfer.

When the user tries to copy a file to removable media, the endpoint client intercepts the transaction and sends the file through the adapter for analysis. If the action is set to Encrypt, the endpoint client encrypts the file using a key deployed by the endpoint profile. The encrypted file can then be opened on any endpoint, assuming that endpoint has the relevant encryption key.

You must define an encryption key for each endpoint profile. Websense Data Security includes one default encryption key. Note that each endpoint might have different encryption keys, based on the profile it belongs to.

✓ **Note**

The default profile contains a default key based on the password of the administrator user that installed Websense Data Security.

To create an encryption key:

1. Select the **Encryption** tab.
2. Click **New**.
3. Enter a password and confirm it.
4. Enter a description, for example ‘Encryption key for March.’
5. Click **OK**.

A code is generated based on the password that you entered, and the key appears on the Encryption tab with Pending status. It remains as pending until you click **Deploy** to deploy the settings to the endpoint servers. While a pending key is awaiting deployment, you cannot generate any more keys.

There can be only one active encryption key for each endpoint profile and 9 enabled keys in the archive. (There is no limit to the number of disabled archived keys.)

After deployment the pending key becomes the active key, and the former active key changes status to decryption-only and appears in the Archived Keys list to be used for files previously encrypted by that key.

> **Note**
> If you want to use the same encryption key in more than one endpoint profile, use the same password in both profiles to generate the keys.

From this screen you can also do the following:

- To disable a decryption-only key, select the key and click **Disable**. You can disable only decryption-only keys. Please note that the change takes place only after:
  a. You deploy the settings
  b. The endpoint receives the change (how often is configurable)
  c. The endpoint is restarted OR the relevant removable media is disconnected from the endpoint
- To enable a disabled key, select the key and click **Enable**. The key reverts to decryption-only status.
- To delete a pending key, click **Delete**. You can delete only pending keys.

Websense recommends you back up your encryption keys every time you modify them. For this reason, whenever you make changes to the Encryption tab, the following alert displays:

```
You have modified your encryption keys. Click Backup to back
up the keys to an external file (strongly recommended).
```

To back up your keys:

1. Click **Backup**.
2. Browse to the location where you want to save the backup file.
3. Click **Save** to close the Save As windows.
4. Click **Close** to close the alert.

> **Note**
> You can also backup your encryption keys by selecting **Encryption Keys** > **Backup** from the Endpoint Profile toolbar.

Rearranging endpoint profiles

Related topics:

- *Adding an endpoint profile*, page 282
- *Deploying endpoint profiles*, page 288

The order of the endpoint profiles in the list affects the order in which they are applied to any endpoint clients that are assigned to multiple profiles. Only the top-level profile is applied.

✓ **Note**
The default profile always appears at the bottom of the profile list and you cannot change its placement.

To rearrange profiles:

1. Select **Settings** > **Deployment** > **Endpoint**.
2. Click **Rearrange Profiles**.
3. In the Rearrange Endpoint Profiles window, select a profile name and use the up and down arrow buttons to move the profile up or down the list.
4. Click **OK**.

   The endpoint profiles list is updated to show the profiles in the order you have selected.

Deploying endpoint profiles

Related topics:

- *Reviewing and deploying changes*, page 22

Once you have defined all the settings for an endpoint profile, the profile can be deployed to the Websense endpoints.

To deploy an endpoint profile:

1. In TRITON - Data Security, click **Deploy**.
2. Click **Yes** to confirm the deployment.
3. The Deployment Status screen appears, showing the progress of the deployment. For more information about this screen, see *Viewing deployment status*, page 203.

Backing up encryption keys

Related topics:

- *Encryption tab*, page 286
- *Restoring encryption keys*, page 289

When Websense Data Security is installed, it includes one default encryption key for use with endpoint profiles. Websense recommends that you back up this key, and any subsequent keys that you create, to an external file. If there is a system crash, you can restore any files that were encrypted on endpoints using these keys.

To back up encryption keys:

1. Select **Settings** > **Deployment** > **Endpoint**.
2. Click the down arrow next to **Encryption Keys**, then click **Backup**. A pop-up window appears.
3. Click **Backup** in the pop-up window.
4. Browse to the location where you want to save the backup file.
5. Click **Save**.
6. Click **Close**.

The file is saved in a Websense-proprietary format. You cannot edit it.

Restoring encryption keys

Related topics:

- *Encryption tab*, page 286
- *Backing up encryption keys*, page 289

If you restore encryption keys from an external file, the restored keys are added to all endpoint profiles as disabled keys. For more information on managing keys in endpoint profiles, see *Encryption tab*, page 286.

To restore encryption keys:

1. Select **Settings** > **Deployment** > **Endpoint**.
2. Click the down arrow next to **Encryption Keys**, then click **Restore**.
3. Click **Browse** and navigate to the location of your backup file.
4. Click **Open**.
5. Click **OK**.

After you restore encryption keys, you must generate a new active key for each profile. In addition, you must enable the restored keys. For example, say profile A has key A1 and profile B has key B1.When you restore keys, both profiles are given 2 disabled keys (A1 and B1).

You need to create a new active key for each profile (for example, A2 and B2) and enable the former keys for decryption only so that those profiles are able to open documents that were encrypted earlier. After you generate new active keys and enable the former keys, your profiles would look like this:

Profile A:

- Key A1 - Decrypt only
- Key B1 - Disabled
- Key A2 - Active

Profile B:

- Key A1 - Disabled
- Key B1 - Decrypt only
- Key B2 - Active

To generate a new active key:

1. Open each endpoint profile, one at a time.
2. Navigate to the **Encryption** tab.
3. In the Active Key section, click **New**.
4. Enter and confirm a password for the key.
5. Click **OK**.

To enable former keys as decryption only:

1. In the Archived Keys section, select each disabled key, one by one, and click **Enable**.
2. Click **OK**.
3. Do this for each endpoint profile.
4. Click **Deploy**.

Configuring endpoint settings

You can define a number of global settings for endpoints, such as how often to test connectivity and check for updates, how much disk space to use for system files, and the action to take when user confirmation is required but not attained.

To access these settings, either click **Settings** on the Endpoint Deployment screen, or select **Settings** > **System** > **Endpoint**.

For more information on configuring endpoint settings, see *Configuring endpoints*, page 214.

Monitoring endpoint removable media

Related topics:

- *Viewing contained files*, page 295

You can monitor or prevent sensitive information being written from an endpoint to a removable device, such as a USB flash drive, CD/DVD, or external hard disk. By default, all devices are monitored.

If you want to target a specific device, follow these steps:

Add the device to the resources list:

1. Select **Main** > **Policy Management** > **Resources**.
2. Under Endpoint, click **Devices**.
3. Click **New**.

For more information, see *Defining Resources*, page 101.

Add the new resource to your endpoint policy:

1. Select **Main** > **Policy Management** > **Data Usage Policies**.
2. Do one of the following:
   - Click a policy and select **New** > **Rule**
   - Click a rule and select **Edit**
3. Go to the **Destination** section for the rule.
4. Select **Endpoint Removable Media**, and click **Edit**.
5. Select Devices from the **Display** drop-down list.
6. Choose the devices to monitor for this policy, by selecting the device and clicking the > button to move it to the **Selected** list.
7. Click **OK**.

Selecting endpoint destination channels to monitor

As well as removable media, you can set up a rule to monitor and analyze endpoint data sent to other destination channels. For example, you can check Web traffic, and software applications on the endpoint.

To select endpoint destinations for monitoring:

1. Select **Main** > **Policy Management** > **Data Usage Policies**.
2. Do one of the following:
   - Click a policy and select **New** > **Rule**
   - Click a rule and select **Edit**
3. Go to the **Destination** section for the rule.
4. You can select from the following:
   - **Web** - Select **Endpoint HTTP/HTTPS** from the **Advanced** drop-down list to monitor endpoint devices such as laptops, and protect them from posting sensitive data to the Web. You can monitor traffic when endpoints are not connected to the network.
   - **Endpoint application** - You can monitor or prevent sensitive data from being copied and pasted from an application such as Microsoft Word, or even downloaded from a browser. This is desirable, because endpoint clients are often disconnected from the corporate network and can pose a security risk.

     If you choose to analyze all activities on a rule's condition page and then select browsers here, this is akin to analyzing all Web content that is downloaded to endpoints. To prevent performance degradation:

     - When files are saved to the browser's cache folders, the crawler analyzes only .csv, .xls/xlsx, .pdf, .txt, and .doc/.docx files.
     - When files are saved to any other local folder, it analyzes all file types.

     Data Security supports the following browsers for endpoint application control: Internet Explorer browsers version 6, 7, and 8. Mozilla Firefox is not supported.

     Note

     If a user's browser is open, new endpoint policies are not enforced on those browsers. Users must close and reopen their browser for new policies to take effect.

   - **Endpoint removable media** - You can monitor or prevent sensitive data from being transferred to removable media. Define the devices to analyze.
   - **Endpoint LAN** - Users commonly take their laptops home and then copy data through a LAN connection to a network drive or share on another computer. They also commonly take data from a shared folder (at work) to copy onto their laptop. With Websense Data Security:

     - You can specify a list of IPs, host names, or IP networks of computers that are allowed as a source or destination for LAN copy.
     - You can intercept data from or to an endpoint client.
     - You can set a different behavior according to the endpoint type (laptop or other) and location (connected or not connected).

     Endpoint LAN control is applicable to Microsoft sharing only.

For more information on monitoring destinations and protecting data on endpoints, see *Rule Wizard - Destination*, page 59.

Bypassing endpoint clients

Related topics:

- *Disabling an endpoint client*, page 294

In certain circumstances, you may want to temporarily disable the endpoint client on a user's computer. Disabling an endpoint client means that no content traffic on that endpoint is analyzed, and if there is a policy breach, content is not blocked.

To disable an endpoint client:

1. Instruct the user on the endpoint to open the Websense Data Endpoint application and click the **Disable** button. (See *Disabling an endpoint client*, page 294 for details.)
2. The dialog that appears contains a bypass ID. Have the end user report it to you.
3. In TRITON - Data Security, select **Main** > **Status & Logs** > **Endpoint Status**.
4. Select the endpoint you want to disable.
5. Click **Bypass Endpoint**.
6. In the Bypass Endpoint window, enter the bypass ID supplied by the end user.
7. Define the amount of time, in days, hours, and minutes, for which the endpoint client should be disabled.
8. Click **Generate Code**. A bypass code is displayed in the field.
9. Send the bypass code to the user.
10. Tell the user to type the code into the screen on the endpoint from step 2 and click **Enter**.

If the user is in stealth mode, this entire procedure can be done by using command-line programs on the endpoint. See the Data Security Deployment Guide for details.

Using the endpoint client software

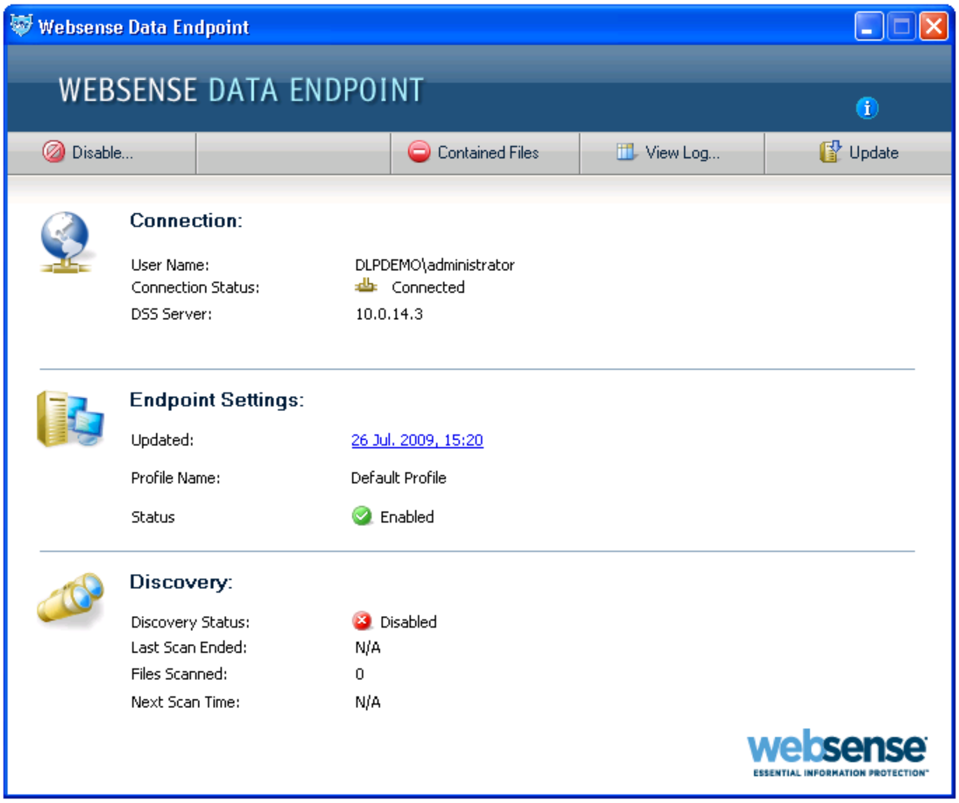
Related topics:

- *Disabling an endpoint client*, page 294
- *Viewing contained files*, page 295
- *Viewing logs*, page 296
- *Updating the endpoint client*, page 297

This section is for end users of a machine where the endpoint client is installed.

When the Websense Data Security endpoint client is installed, an icon appears on the endpoint machine’s task bar. The icon indicates whether the machine is protected or unprotected/bypassed.

The end user can click this icon for status information:



Connection:

User Name:	DLPDEMO\administrator
Connection Status:	Connected
DSS Server:	10.0.14.3

Endpoint Settings:

Updated:	26 Jul. 2009, 15:20
Profile Name:	Default Profile
Status	✓ Enabled

Discovery:

Discovery Status:	✗ Disabled
Last Scan Ended:	N/A
Files Scanned:	0
Next Scan Time:	N/A

On this screen you can:

- see whether the machine is connected to an endpoint server, and check the IP address of the Data Security server
- view the endpoint profile name, and when it was last updated
- view the discovery status, and details of the last and next discovery scans

✓ **Note**

This screen is available only if **Interactive mode** is selected on the Properties tab of the endpoint profile.

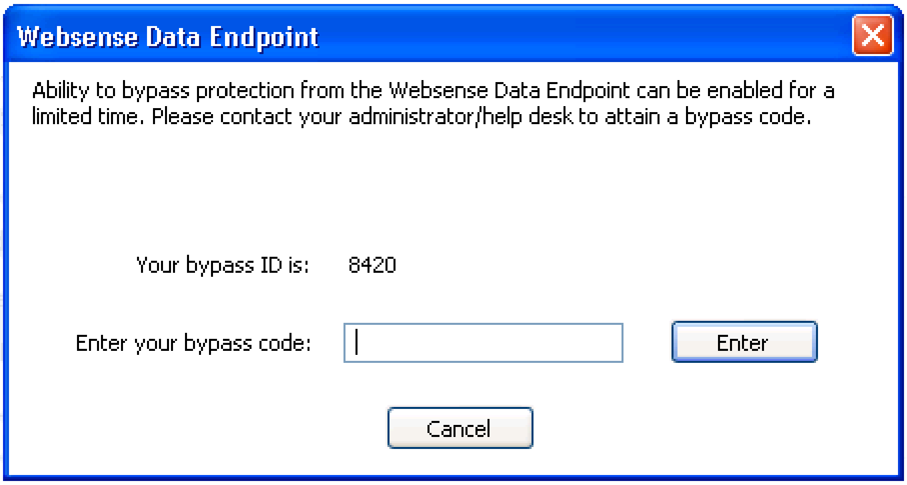
Disabling an endpoint client

Related topics:

- *Bypassing endpoint clients*, page 293

If you want to temporarily disable the endpoint client on a user's computer, first follow the instructions in *Bypassing endpoint clients*, page 293. The end user then does the following:

1. On the Websense Data Endpoint screen, click **Disable**.



Ability to bypass protection from the Websense Data Endpoint can be enabled for a limited time. Please contact your administrator/help desk to attain a bypass code.

Your bypass ID is: 8420

Enter your bypass code:

2. Report the bypass ID to the Data Security administrator.
3. Enter the bypass code supplied by the administrator.
4. Click **Enter**.

The client is disabled for the length of time specified when the bypass code was created. The button on the task bar updates from the **Disable** button with the red no entrance icon to an **Enable** button with a green check mark icon.

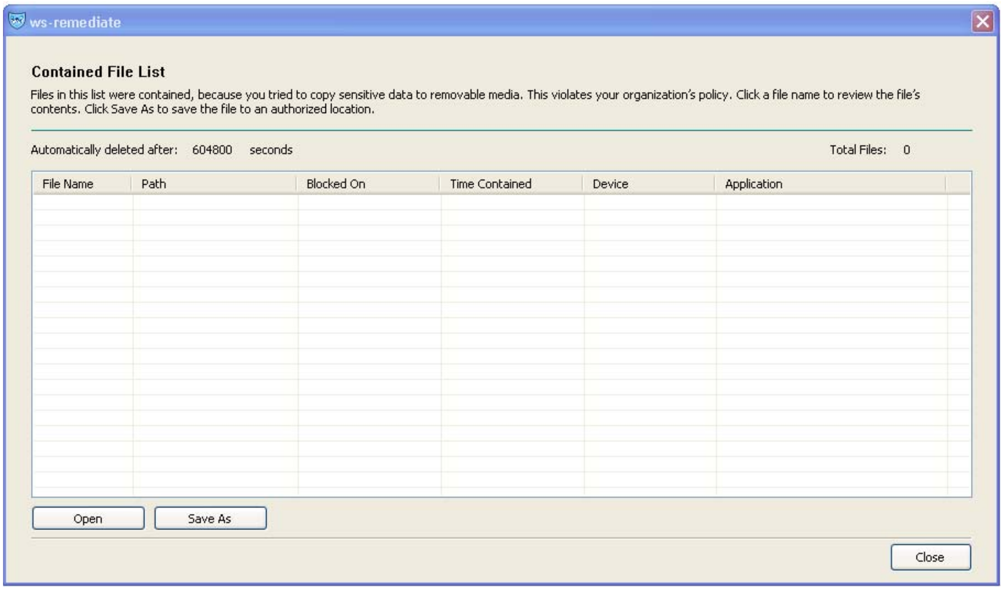
Viewing contained files

Related topics:

- *Monitoring endpoint removable media*, page 291

If you have chosen to prevent sensitive information being written from an endpoint to a removable device, such as a USB flash drive, CD/DVD, or external hard disk, any files that an end user attempts to copy are contained. The user can view the contents of these files from the endpoint client, and choose to save them to an authorized location instead.

1. On the Websense Data Endpoint screen, click **Contained Files**.



Contained File List

Files in this list were contained, because you tried to copy sensitive data to removable media. This violates your organization's policy. Click a file name to review the file's contents. Click Save As to save the file to an authorized location.

Automatically deleted after: 604800 seconds

Total Files: 0

File Name	Path	Blocked On	Time Contained	Device	Application

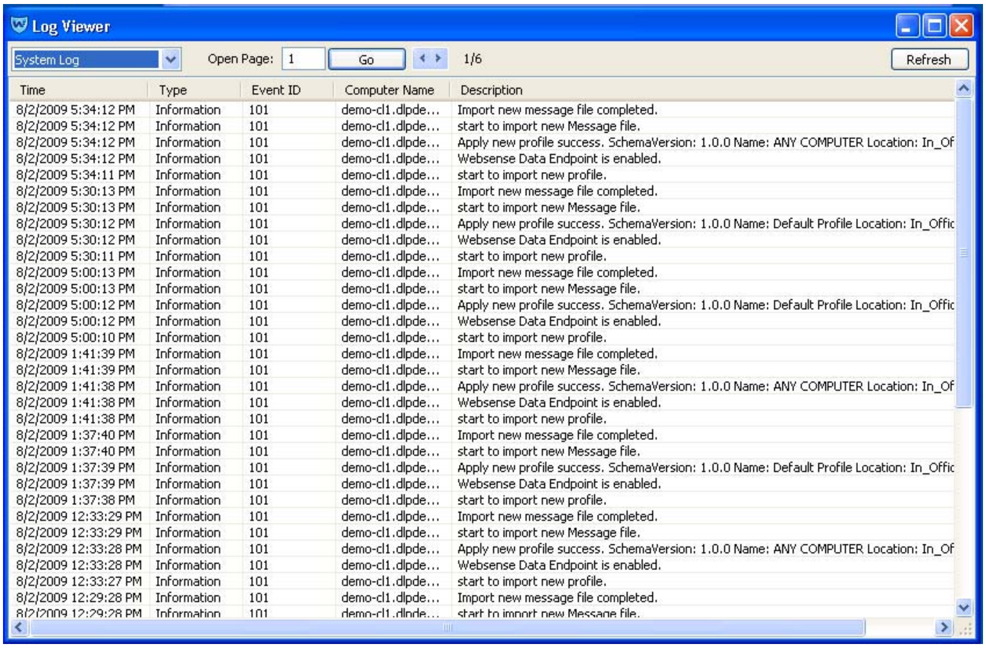
2. To see the contents of a file, select the file and click **Open**.
3. To save a file to an authorized location, select the file and click **Save As**, then browse to the new location.
4. Click **Close** when done.

Viewing logs

There are two logs available in the endpoint client:

- The system log contains information about changes on the endpoint machine, for example:
  - changes of connection status, such as a machine moving from an office to a remote location
  - when the Websense Data Endpoint is enabled or disabled
  - when endpoint profiles are applied and updated
  - when the client is connected to or disconnected from the endpoint server
- The content log contains details of file operations that have been picked up by the endpoint policy, and any actions taken by the endpoint as a result.

To see the log details, on the Websense Data Endpoint screen, click **View logs**.



Time	Type	Event ID	Computer Name	Description
8/2/2009 5:34:12 PM	Information	101	demo-cl1.dlpde...	Import new message file completed.
8/2/2009 5:34:12 PM	Information	101	demo-cl1.dlpde...	start to import new Message file.
8/2/2009 5:34:12 PM	Information	101	demo-cl1.dlpde...	Apply new profile success. SchemaVersion: 1.0.0 Name: ANY COMPUTER Location: In_Of
8/2/2009 5:34:12 PM	Information	101	demo-cl1.dlpde...	Websense Data Endpoint is enabled.
8/2/2009 5:34:11 PM	Information	101	demo-cl1.dlpde...	start to import new profile.
8/2/2009 5:30:13 PM	Information	101	demo-cl1.dlpde...	Import new message file completed.
8/2/2009 5:30:13 PM	Information	101	demo-cl1.dlpde...	start to import new Message file.
8/2/2009 5:30:12 PM	Information	101	demo-cl1.dlpde...	Apply new profile success. SchemaVersion: 1.0.0 Name: Default Profile Location: In_Offic
8/2/2009 5:30:12 PM	Information	101	demo-cl1.dlpde...	Websense Data Endpoint is enabled.
8/2/2009 5:30:11 PM	Information	101	demo-cl1.dlpde...	start to import new profile.
8/2/2009 5:00:13 PM	Information	101	demo-cl1.dlpde...	Import new message file completed.
8/2/2009 5:00:13 PM	Information	101	demo-cl1.dlpde...	start to import new Message file.
8/2/2009 5:00:12 PM	Information	101	demo-cl1.dlpde...	Apply new profile success. SchemaVersion: 1.0.0 Name: Default Profile Location: In_Offic
8/2/2009 5:00:12 PM	Information	101	demo-cl1.dlpde...	Websense Data Endpoint is enabled.
8/2/2009 5:00:10 PM	Information	101	demo-cl1.dlpde...	start to import new profile.
8/2/2009 1:41:39 PM	Information	101	demo-cl1.dlpde...	Import new message file completed.
8/2/2009 1:41:39 PM	Information	101	demo-cl1.dlpde...	start to import new Message file.
8/2/2009 1:41:38 PM	Information	101	demo-cl1.dlpde...	Apply new profile success. SchemaVersion: 1.0.0 Name: ANY COMPUTER Location: In_Of
8/2/2009 1:41:38 PM	Information	101	demo-cl1.dlpde...	Websense Data Endpoint is enabled.
8/2/2009 1:41:38 PM	Information	101	demo-cl1.dlpde...	start to import new profile.
8/2/2009 1:37:40 PM	Information	101	demo-cl1.dlpde...	Import new message file completed.
8/2/2009 1:37:40 PM	Information	101	demo-cl1.dlpde...	start to import new Message file.
8/2/2009 1:37:39 PM	Information	101	demo-cl1.dlpde...	Apply new profile success. SchemaVersion: 1.0.0 Name: Default Profile Location: In_Offic
8/2/2009 1:37:39 PM	Information	101	demo-cl1.dlpde...	Websense Data Endpoint is enabled.
8/2/2009 1:37:38 PM	Information	101	demo-cl1.dlpde...	start to import new profile.
8/2/2009 12:33:29 PM	Information	101	demo-cl1.dlpde...	Import new message file completed.
8/2/2009 12:33:29 PM	Information	101	demo-cl1.dlpde...	start to import new Message file.
8/2/2009 12:33:28 PM	Information	101	demo-cl1.dlpde...	Apply new profile success. SchemaVersion: 1.0.0 Name: ANY COMPUTER Location: In_Of
8/2/2009 12:33:28 PM	Information	101	demo-cl1.dlpde...	Websense Data Endpoint is enabled.
8/2/2009 12:33:27 PM	Information	101	demo-cl1.dlpde...	start to import new profile.
8/2/2009 12:29:28 PM	Information	101	demo-cl1.dlpde...	Import new message file completed.
8/2/2009 12:29:28 PM	Information	101	demo-cl1.dlpde...	start to import new Message file.

To see the latest log information, click **Refresh**.

Updating the endpoint client

Endpoint clients check for updates at intervals specified in the endpoint global settings. For more information on configuring endpoint settings, see *Configuring endpoint settings*, page 290.

The end user can start an update check at any time by clicking **Update** on the Websense Data Endpoint screen.

16 Troubleshooting

Networks are complex, and because of the vast disparities in their composition (and their propensity toward change), there can be occasional glitches in the installation and maintenance of network-centric software. Websense goes to great pains—including continuing product refinement—to ensure the easy installation and maintenance of our software, but problems can arise.

This chapter discusses the conditions, circumstances and resolution of issues that might occur in your use of the data security products, as well as provides contact points for full support.

Problems and Solutions

Related topics:

- *Discovery*, page 300
- *Endpoint*, page 301
- *Fingerprinting*, page 302
- *Incidents*, page 304
- *Miscellaneous*, page 305
- *Performance*, page 306
- *Printer agent*, page 307
- *Protector*, page 308
- *Linking*, page 309

This section lists common problems and their solutions. See the Related Topics box to choose a specific area of concern.

Discovery

Related topics:

- *Difficulty locating network shares*, page 300
- *Discovery is configured to discover sensitive files but sensitive files are not found*, page 300

This section lists problems related to discovery and their solutions. See the Related Topics box to choose a specific area of concern.

Difficulty locating network shares

If the protector is having trouble locating your shares during network discovery:

1. Run the following command on the protector in order to list the desired share:

   ```
   cifsls --list /<sharename> -h <servername\ip> -d <domain> -u
   <username> -p <password>
   ```

   You can add -t <1-10> to get verbose output. This command can give you a good idea of the problem’s origin.
2. Make sure you can access the share from a Windows machine.
3. Make sure there’s no problem with the share itself.
4. Refer to the following protector logs:
   - /opt/pa/log/crawler.log — Discovery jobs log
   - /opt/pa/log/crawlerd.log
   - /opt/pa/log/cifsd.log — This log shows remote access issues, such as permissions, to the scanned machines.
5. Confirm if the credentials used by the protector appliance are working. See knowledge-base article “DSS—Verify authentication from protector (command line) for Network Discovery.”

For other ideas, see knowledge-base article “Network Discovery Troubleshooting.”

Discovery is configured to discover sensitive files but sensitive files are not found

It could be that the Data Security server is not on the domain, thus it does not have rights to shares on other machines on the domain. The only way to alleviate this would be to either launch TRITON - Data Security from a machine on the domain, logged in with an account that has rights to view shares, or add the Data Security server to the domain.

Endpoint

Related topics:

- ◆ *User name does not display on endpoint list in TRITON - Data Security*, page 301
- ◆ *Endpoint shield does not display on the client computer*, page 301
- ◆ *Failed to deploy endpoint configuration*, page 302

This section lists problems related to endpoint deployments and their solutions. See the Related Topics box to choose a specific area of concern.

User name does not display on endpoint list in TRITON - Data Security

The Websense Data Endpoint requires the Terminal Services service to be enabled and set to **Manual** to report user names back to the endpoint agent service.

1. On the endpoint machine for the missing user, open Windows Control Panel and select **Administrative Tools** > **Services**.
2. Locate the Terminal Services service. Double-click it.
3. Change the service’s Startup type from **Disabled** or **Automatic** to **Manual.**
4. Click **OK**.
5. Reboot the computer.

The user name should properly be displayed on the endpoint list once the endpoint has rebooted.

Endpoint shield does not display on the client computer

The Websense Data Endpoint requires the Terminal Services service to be enabled and set to **Manual** to display its icon.

1. On the endpoint machine for the missing user, open Windows Control Panel and select **Administrative Tools** > **Services**.
2. Locate the Terminal Services service. Double-click it.
3. Change the service’s Startup type from **Disabled** or **Automatic** to **Manual.**
4. Click **OK**.
5. Reboot the computer.

The endpoint shield should now display properly.

Failed to deploy endpoint configuration

Occasionally, the endpoint server on your Data Security Server(s) may fail to deploy and you may receive this error:

```
Failed to deploy endpoint configuration. The endpoint
configuration is not valid or the endpoint profile [Default
Profile] does not contain an active or pending encryption
key.
```

This error could result from several conditions:

- You restored your encryption keys but neglected to recreate an active key for each endpoint profile. After you restore encryption keys, you must generate a new active key for each profile.
- You forgot to deploy the new active keys. You must click **Deploy** any time you generate a new active key for a profile.
- You forgot to enable any disabled keys that were added during the restore process. Restored keys are added in a disabled state. You must enable them for them to take effect.

See *Restoring encryption keys*, page 289 for instructions on how to perform these actions.

Fingerprinting

Related topics:

- *File has no fingerprint*, page 303
- *Validation script timeout*, page 303
- *No connectivity to fingerprint database*, page 303
- *Other fingerprinting errors*, page 303

This section lists problems related to fingerprinting and their solutions. See the Related Topics box to choose a specific area of concern.

You can monitor the status and view fingerprinting errors in TRITON - Data Security.

Error details appear in the Status column when you select either:

Main > Policy Management> Content Classifiers > PreciseId Fingerprinting - Files and Directories

or

Main > Policy Management > Content Classifiers > PreciseId Fingerprinting - Files and Directories > PreciseID Fingerprinting - Database Records

More detailed error messages appear in the log files: PAFastKeyPhrases log and fprep.log.

File has no fingerprint

This error occurs when a file selected for files and directory fingerprinting is too small to be fingerprinted. To scan this file, reset the file size limit in TRITON - Data Security.

1. Select **Main** > **Policy Management> Content Classifiers** > **PreciseId Fingerprinting - Files and Directories**.
2. Navigate to the **File Filtering** tab.
3. Change parameters in the **Filter by Size** section of the screen.
4. Click **OK**.

Validation script timeout

During a database fingerprinting scan, if the crawler finds a script matching the name of your fingerprinting classifier, <classifier-name>_validation.[bat|exe|py], it runs that script.

If it does not, it searches for a default script, default_validation.[bat|exe|py], and runs that.

If neither exists, it does not perform validation.

If you are getting validation script timeout errors, you can disable the script by renaming it.

See *Creating a validation script*, page 91 for more information on validation scripts.

No connectivity to fingerprint database

Connectivity to a PreciseID Fingerprint repository has been lost. Fingerprint repositories are located on all Data Security servers and protectors. Additional repositories can be located on network servers.

1. Check to see if all servers and protectors are powered on.
2. Open a command prompt and try to ping the affected server from the Data Security Management Server.
3. Check that credentials were supplied correctly.

Other fingerprinting errors

1. Try opening a file share from the Crawler machine.
2. Check PANTFSMonitor logs on the Crawler machine:
   - Certain files may be too large (> 20 Mbytes)
   - File may be in use (Error code 5 or 32)
   - Access to directory can be denied (Error code 5)
3. Open the Properties for the policy and make sure you can view Sample Data.

If the database is under heavy use, try to fingerprint a replica.

Incidents

Related topics:

- *Cannot clear data out of Data Discovery Dashboard even when incidents are set to ignored*, page 304
- *Event log shows audited events, but no incident is created*, page 304
- *Incident export lacks Data Discovery incidents*, page 305
- *NLP policy isn't being triggered, and events are undetected*, page 305

This section lists problems related to incidents and reporting and their solutions. See the Related Topics box to choose a specific area of concern.

Cannot clear data out of Data Discovery Dashboard even when incidents are set to ignored

Try deleting the incidents rather than ignoring them. Select **Main** > **Data Discovery** > **Incidents**.

To delete a single incident, locate the incident in question and click the box on the far-left side. Locate the red **X** in the tool bar. Click it and select **Delete Selected Incidents**.

To delete multiple incidents, use the display and column filters as appropriate so that only the incidents you desire to delete are displayed. Select all displayed incidents.

Click the red **X** in the tool bar and select **Delete Selected Incidents**.

This should clear the incidents from the dashboard summary.

Event log shows audited events, but no incident is created

There are a few possible causes for this issue:

- If there are any off-box components in the Data Security installation and the Data Security servers are not on the domain, then all passwords and user names must match for the service accounts being used for Data Security.

  For example, if the account Websense with a password of “Pa55word123” is being used as the service account on TRITON - Data Security, then the service account in use for any off-box Data Security-installed components must also be Websense with the password of “Pa55word123” as well.

  If the user names and passwords do not match, then the off-box components will be unable to communicate with the shared directories of the Data Security Management Server, which will prevent incidents from being recorded to the archive folder on the Data Security Management Server.

- Incidents queued on the server performing analysis of the events. This is actually a delay of incidents being loaded into the Oracle database. Incidents eventually appear from audited events; however, there can be a severe lag time between the actual event and the incident being displayed. See the knowledge-base article "High Queues on a Data Security Server Policy Engine" for how to resolve this issue.

Incident export lacks Data Discovery incidents

This is expected behavior. Incident export exports only data usage and endpoint incidents.

NLP policy isn't being triggered, and events are undetected

Some events that are submitted for analysis do not trigger policies. Typically, these are NLP or complex policies that use compiled Python scripts. Websense may not be in your system's pythonpath variable, and NLP uses python. See knowledge-base article "Some events don't appear to trigger incidents when they should" for instructions on modifying the path.

Miscellaneous

Related topics:

- *Failed user directory import*, page 305
- *Wrong default email address displays*, page 306
- *Error 400, bad request*, page 306
- *Invalid Monitoring Policy XML File*, page 306

This section lists miscellaneous problems and their solutions. See the Related Topics box to choose a specific area of concern.

Failed user directory import

There are a few reasons why the user directory import might fail, such as access problems or an incorrect file structure in the import file. If the import fails, there is a **Failed** link in the Status column on the import screen.Take these steps in TRITON - Data Security:

1. Click the **Failed** status link to access and read the user directory import log.
2. Select **Settings** > **System** > **User Directories** then choose your user directory and examine the IP address and port settings. If you have access problems, it's likely you didn't supply the correct IP or port for the user directory server.
3. If the problem is an incorrect CSV file structure, follow these instructions from Chapter 11, *Importing user entries from a CSV file*, page 218.

Wrong default email address displays

When forwarding events to another user, the email comes from email@mycompany.com rather than a valid email address. To resolve this:

1. In TRITON - Data Security, select **Settings** > **Authorization** > **Administrators**.
2. Select the account you to edit.
3. Modify the email address field.
4. Click **OK**.
5. Log off.
6. Log on again.

Error 400, bad request

Data Security analyzed an HTTP request and determined you do not have sufficient system resources for transactions of this size. See the knowledge-base article “Data Security — Large Transactions are Not Recognized” for instructions on removing transaction size limitations.

Invalid Monitoring Policy XML File

This error sometimes appears when you select **Settings** > **Deployment** > **System Modules** and click the protector. Rather than the edit dialog displaying, you get the error message instead. This typically happens when the policy XML file sent by the protector is inconsistent when compared to the server schema.

For a solution, refer to the knowledge-base article “Invalid Monitoring Policy XML File error when attempting to access protector settings.”

Performance

Related topics:

- *Discovery and fingerprinting scans are slow*, page 306

This section lists problems related to performance and their solutions. See the Related Topics box to choose a specific area of concern.

Discovery and fingerprinting scans are slow

Do you have external antivirus software? If so, configure it to exclude the following directories from antivirus scanning on all Data Security servers and Data Security Management Servers:

- :\Program Files\Websense\*.*
- :\Oracle\*.* *:\Program files\Oracle\*.*

- :\Program files\Microsoft SQL Server*.*
- :\Inetpub\mailroot\*.*
- :\Inetpub\wwwroot\*.*
- %TEMP%*.*
- %WINDIR%\Temp\*.*

See your AV software documentation for instructions. On non-management servers, such as Data Security Server policy engines, exclude the following directories from anti-virus scanning:

- :\Program Files\Websense\*.*
- :\Inetpub\mailroot\*.*
- :\Inetpub\wwwroot\*.*
- %TEMP%*.*
- %WINDIR%\Temp\*.*

This should improve system performance. If you are not running antivirus software, contact Websense Technical Support (see below) for help in improving performance.

Printer agent

Related topics:

- *No events from printer agent*, page 307

This section lists problems related to the printer agent and their solutions. See the Related Topics box to choose a specific area of concern.

No events from printer agent

Check the printer agent's log (change to "debug" if necessary). The log is located on the print server at \Websense\Data Security\DSSPrinterAgent.

Make sure the Print Processor is set to "DSSPrinterAgent." Test the printer agent with the Windows HP LaserJet 5 driver to see if the problem is with the third-party driver or with the printer agent itself.

We recommend that both your Data Security server and the printer agent reside on a domain, and share the same service account. If one of the printers is out of the domain, make sure there are no permissions issues between the printer agent and the Data Security server; use the same service account user name and password.

If you need to contact Websense Technical Support about printer agent issues, be sure to have a copy of the the PDF and .spl files, the printer model, driver used, driver type (PCL, PostScript), driver version and what type of information is to be detected.

Protector

Related topics:

- *Firefox Portable (and other browsers) won't detect fingerprinted files sent via Hotmail, Gmail and other Web-based email*, page 308
- *Protector authentication problems*, page 308

This section lists problems related to the protector and their solutions. See the Related Topics box to choose a specific area of concern.

Firefox Portable (and other browsers) won't detect fingerprinted files sent via Hotmail, Gmail and other Web-based email

Sometimes if you attach a fingerprinted file to an email using Web-based email, the attachment is not detected during analysis. The attached file does not appear in the Analyzed Files or DetectorTemp directories; the protector is not sending the file for analysis.

If these files are going undetected, take these steps to remedy the situation:

1. Go to **Settings > Deployment > System Modules**.
2. Click the **protector**.
3. In the **Edit ICAP** dialog, select the **HTTP** tab.
4. Change the Minimum transaction size to 5 bytes.
5. Click **OK**.

Protector authentication problems

You have set credentials in the Data Security management interface, but Network Discovery is still failing. You need to confirm if the credentials used by the protector appliance are working.

- See knowledge-base article "DSS—Verify authentication from protector (command line) for Network Discovery."

Linking

Related topics:

- *Linking Service information is not shown on the Linking page*, page 309
- *Websense Linking Service stopped responding*, page 309
- *System alerts that linking has not been configured*, page 310
- *Unable to connect to TRITON - Web Security*, page 310
- *Buttons in TRITON security center module tray return error*, page 311

This section lists problems related to linking and the Websense Linking Service and their solutions. See the Related Topics box to choose a specific area of concern.

Linking Service information is not shown on the Linking page

If you do not see information about the Websense Linking Service on TRITON - Data Security's Linking page, it means that the Linking Service was never installed. Typically, the Linking Service is installed as part of a custom Web Security installation on a Windows machine.

When you configure linking, the system attempts to install the Linking Service automatically. If Web Security's Policy Server is running on Windows, the Linking Service is installed on this machine. If not, it is installed on the Log Server machine.

If the Policy Server is running on Linux and TRITON - Web Security does not have access to a Log Server with its own Policy Server, then the Linking Service cannot be auto-installed, and you will not see Linking Service information on the TRITON - Data Security Linking page.

To resolve this, you must add the Websense Linking Service manually to a Windows server (using the Web Security custom installation). Then, when you configure linking, TRITON - Data Security looks for the Websense Linking Service and enables it. It displays the IP address and port number for the Linking Service that it found in the Linking Service section of the screen.

Alternatively, you can install Log Server, retry Linking, and auto-install the Linking Service as described above.

Websense Linking Service stopped responding

In TRITON - Data Security, take these steps:

1. Choose **Settings** > **Configuration** > **System** > **Linking**
2. Click **Edit** under Linking Service.
3. Make sure the **Enabled** check box is selected.

4. Click **Update** to retrieve the latest host and port settings of the linking service. These settings can change.

System alerts that linking has not been configured

When your Websense software subscription includes both Web and data security, you have the option to link the 2 security solutions. A system alert appears on the Today page in TRITON - Data Security when your subscription allows linking, but it has not been configured.

When you configure linking:

- Data security software gains access to user data gathered by Web security components.
- Data security software can access Master Database categorization information.
- Administrators can be given seamless access to both the Web Security and the Data Security modules of the TRITON Unified Security Center.
- To configure linking between your Web and data security solutions, go to the **Settings** > **System** > **Linking** page in TRITON - Data Security.

Unable to connect to TRITON - Web Security

If you receive an error when you try to connect to TRITON - Web Security from TRITON - Data Security, either a configuration or a communication problem is likely at fault.

To troubleshoot this problem, first check to see if you can open TRITON - Web Security directly. To do this, open a Web browser on the machine that you are currently using to access TRITON - Data Security, and then enter the TRITON - Web Security URL and port in the address bar. For example:

```
https://<IP address>:9443/mng/
```

Replace <*IP address or name*> with the IP address or fully qualified domain name of the TRITON - Web Security machine.

- If you are able to connect directly, go to the **Settings** > **System** > **Linking** page in TRITON - Data Security and verify that the IP address or host name provided matches the one that you used to connect directly to TRITON - Web Security.

  Note that the connection port entered on the Linking page (by default, 7443) is not the same port used when you access TRITON - Web Security directly.
- If you cannot connect directly, there may be a network communication problem, or a problem on the TRITON - Web Security machine.
  - Make sure that the TRITON - Web Security machine is on.
  - Use the Windows Services dialog box to verify that the TRITON - Web Security service has started.
  - Check the Windows Event Viewer on the TRITON - Web Security machine for errors from the Data Security Management Server.

- Use the **ping** utility to verify that the TRITON - Web Security machine can connect to the TRITON - Data Security machine.
- If ping shows that data can be passed between the machines, use the **telnet** utility to verify that the linking port (7443, by default) is open between the 2 machines.
- Check the Windows Event Viewer on the TRITON - Data Security machine for errors from Linking Service.

Buttons in TRITON security center module tray return error

If you receive an error when you click **Web Security** in TRITON - Data Security, the administrator account that you use to log on to TRITON - Data Security may not have been granted permission to access TRITON - Web Security. In order to change between TRITON Unified Security Center modules, an administrator must:

- Be given access to each module
- Have the same account type (Websense user or network) in each module
- Have the same user name in each module
- Use the same password to access each module

The default TRITON - Web Security account, **WebsenseAdministrator**, does not have TRITON - Data Security access by default. Likewise, the default TRITON - Data Security account, **admin**, does not have TRITON - Web Security access by default.

Unconditional Super Administrators can configure each administrator’s level of access to modules and features of the TRITON Unified Security Center.

Linking Websense Web Security and Websense Data Security, among other things, connects the Web Security and Data Security modules of the TRITON Unified Security Center.

In order for linking to succeed, your Websense Web Security version must match your Websense Data Security version.

Online Help

Select the **Help** option within the program to display detailed information about using the product.

IMPORTANT

Default Microsoft Internet Explorer settings may block operation of the Help system. If a security alert appears, select **Allow Blocked Content** to display Help.

If your organization's security standards permit, you can permanently disable the warning message on the Advanced tab of the **Tools** > **Internet Options** interface. (Check **Allow active content to run in files on My Computer** under Security options.)

Technical Support

Technical information about Websense software and services is available 24 hours a day at:

www.websense.com/support/

- the latest release information
- the searchable Websense Knowledge Base
- support forums
- support webinars
- show-me tutorials
- product documents
- answers to frequently asked questions
- Top customer issues
- in-depth technical papers

For additional questions, click the **Contact Support** tab at the top of the page.

If your issue is urgent, please call one of the offices listed below. You will be routed to the first available technician, who will gladly assist you.

For less urgent cases, use our online **Support Request Portal** at ask.websense.com.

For faster phone response, please use your **Support Account ID**, which you can find in the Profile section at MyWebsense.

Location	Contact information
North America	+1-858-458-2940
France	Contact your Websense Reseller. If you cannot locate your Reseller: +33 (0) 1 5732 3227
Germany	Contact your Websense Reseller. If you cannot locate your Reseller: +49 (0) 69 517 09347
UK	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Rest of Europe	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Middle East	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Africa	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Australia/NZ	Contact your Websense Reseller. If you cannot locate your Reseller: +61 (0) 2 9414 0033
Asia	Contact your Websense Reseller. If you cannot locate your Reseller: +86 (10) 5884 4200
Latin America and Caribbean	+1-858-458-2940

For telephone requests, please have ready:

- Websense subscription key
- Access to TRITON - Data Security
- Familiarity with your network’s architecture, or access to a person who has this knowledge
- Specifications of the machines running the Data Security Management Server and other Data Security servers
- A list of other applications running on the Data Security Management Server and other Data Security servers

Part IV

Appendices

A Predefined Policies

Predefined policies enable you to quickly and easily define what type of content is considered a security breach on your network.

The predefined policies included in the Websense Data Security are constantly being updated and improved. Many of the Websense Data Security policies are Natural Language Processing (NLP) policies which enable more powerful search and analysis techniques.

While choosing a policy or policy category, some items are set "off" by default, and can be activated individually by checking them according to the specific needs of the organization or business.

Data Usage policies

The predefined data usage policies are based on detection of data types and of regulations. The data type policies are categorized as follows:

- Personally Identifiable Information (PII)
- Private Health Information (PHI)
- Credit Cards
- Financial Data
- Acceptable Use
- Company Confidential and Intellectual Property

The regulation policies are categorized as follows:

- Payment Card Industry (PCI)
- Privacy Regulations
- US and Canada Federal Regulations
- Financial Regulations

Personally Identifiable Information (PII)

The following predefined policies are available for the detection of private information:

- PII policies for 33 countries

  Detects personal information, such as names, dates of birth, driver license numbers, and identification numbers, tailored to specific countries.
- Password Dissemination

  Detects content suspected to be a password in clear text.
- Social Insurance Numbers

  Detects valid Canadian Social Insurance Numbers (SIN).
- Social Security Numbers

  Detects valid US Social Security numbers.

Private Health Information (PHI)

The following predefined policies are available for the detection of private health information:

- Health Data

  Detects data types related to medical conditions and drugs.
- PHI

  5 policies to detect private health information for Israel, USA, Australia, Norway, and United Kingdom.

Credit Cards

The following predefined policies are available for the detection of credit card information:

- Credit Cards

  Detects credit card numbers. Separate policies are available for detecting credit card numbers prevalent in Japan, Israel, Europe, and USA.
- Credit Card Tracks

  Detects credit card magnetic track information.
- Credit Cards for Printer Agent

  Detects credit card numbers obtained from using the printer agent OCR. This takes into account possible OCR errors.

Financial Data

The following predefined policies are available for the detection of financial information:

- Financial Information

  Detects general, personal, and investment financial information. Separate policies are available for detecting financial data specific to Israel, Germany, Netherlands, Switzerland, Norway, Italy, Iceland, France, Poland, UK, Spain, Turkey, Denmark, Sweden, Greece, Finland, and Ireland.

- Mergers and Acquisitions
- Pricing Information
- RTN/ABA Numbers

  Detects Routing Transit Numbers (RTN), also known as American Bankers Association (ABA) numbers.
- ISIN and CUSIP

  Detects an International Securities Identification Number (ISIN), which uniquely identifies a security. The ISIN code is a 12-character alphanumerical code that serves as uniform identification of a security at trading and settlement.
- EIN

  Detects Employer Identification Numbers.

Acceptable Use

The following predefined policies are available for the detection of possible acceptable use transgressions:

- Acceptable Usage - Obscenities & Racism

  Detects offensive or inappropriate terms.
- Database Files
- Email Addresses
- Encrypted Files
- Malicious Concealment

  Detects content suspected to have been manipulated for the purposes of avoiding detection.
- W-2 Forms

  Detects W-2 tax forms.
- Resume for HR

  Detects documents that are resumes (CVs). Separate policies are available to detect resumes in Hebrew, and in Russian or Ukrainian.
- License Keys

  Detects Microsoft license keys, to help mitigate software piracy and unauthorized usage of corporate assets.
- Confidential Warning

  Detects sensitive text in the header, footer, or metadata fields of a document.

Company Confidential and Intellectual Property

The following predefined policies are available for the detection of company confidential or intellectual property data:

- Software Source Code and Design

  Includes policies to detect software design documents and source code such as SPICE and Verilog.
- Energy

  Detects petroleum and gas sensitive information.
- Telecom

  Includes policies to detect serial (IMEI) numbers of cell phones, call detail records, and location coordinates.
- Media

  Detects possible movie manuscripts.
- Strategic Planning Documents
- Business and Technical Drawing Files
- Network Security Information
- Patents

United States Federal and Industry Regulations

The following regulatory compliances are supported by Websense Data Security's predefined policies:

- *Gramm-Leach-Bliley Act (GLBA)*, page 321
- *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, page 321
- *Children's Online Privacy Protection Act of 1998 (COPPA)*, page 322
- *FERPA educational institution student privacy regulation*, page 322
- *Canadian Personal Information Protection and Electronic Documents Act PIPEDA*, page 322
- *Check 21 Act*, page 323
- *FFIEC*, page 323
- *Payment Card Industry (PCI)*, page 323
- *US Securities and Exchange Commission (SEC)*, page 323
- *Sarbanes-Oxley Financial and Accounting Disclosure Information (SOX)*, page 323
- *FISMA*, page 324
- *DIACAP*, page 324
- *FDA - 21 CFR*, page 324
- *FCRA*, page 324
- *MITS*, page 324
- *ITAR*, page 325
- *FERC*, page 325
- *NYSE Rule 472*, page 325

Gramm-Leach-Bliley Act (GLBA)

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, is a US Federal regulation that includes provisions to protect consumers' personal financial information held by financial institutions.

GLBA permits the consolidation of financial services companies and requires financial institutions to issue privacy notices to their customers, giving them the opportunity to opt-out of some sharing of personally identifiable financial information with outside companies. GLBA also governs the disclosure of such personal information.

Statute -- 15 USC, Subchapter I, Sec. 6801-6809 available at http://www.ftc.gov/privacy/glbact/glbsub1.htm (http://www.ftc.gov/privacy/glbact/glbsub1.htm)

Privacy Rule Regulation -- 16 CFR Part 313 available at http://www.ftc.gov/os/2000/05/65fr33645.pdf (http://www.ftc.gov/os/2000/05/65fr33645.pdf)

Safeguard Regulation -- 16 CFR Part 314 available at http://www.ftc.gov/os/2002/05/67fr36585.pdf (http://www.ftc.gov/os/2002/05/67fr36585.pdf)

"Nonpublic personal information" means: (i) Personally identifiable financial information; and (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available. (2) Nonpublic personal information does not include: (i) Publicly available information, except as included on a list described in paragraph (n)(1)(ii) of this section; or (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available. [16 CFR 313.3(n)(1)]

"Personally identifiable financial information" means any information: (i) A consumer provides to you to obtain a financial product or service from you; (ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or (iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer. [16 CFR 313.3(o)(1)]

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act is a US Federal law that specifies a series of administrative, technical, and physical safeguards, organizational and documentation requirements for covered entities to use to assure the availability, confidentiality, and integrity of electronically protected health information.

HIPAA includes provisions designed to streamline the health care businesses by encouraging electronic transactions. HIPAA regulations also require covered entities to protect the security and confidentiality of patient information. Detects combinations of first and last names in proximity to sensitive or common diseases, and DNA sequences.

Citation -- Public Law 104-191 available at http://aspe.hhs.gov/admnsimp/pl104191.htm (http://aspe.hhs.gov/admnsimp/pl104191.htm)

Regulations -- 45 CFR Parts 160 and 164 available at http://www.hhs.gov/ocr/combinedregtext.pdf (http://www.hhs.gov/ocr/combinedregtext.pdf)

Children's Online Privacy Protection Act of 1998 (COPPA)

The Children's Online Privacy Protection Act of 1998 is a U.S. Federal law which applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age. Most of the terms of COPPA apply only to websites and organizations operated for commercial purposes and usually exempt recognized non-profit organizations. The authority to oversee activities related to the management of COPPA rests primarily with the Federal Trade Commission (FTC).

COPPA prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.

Statute -- 15 USC 6501 et seq. available at http://www.ftc.gov/ogc/coppa1.pdf (http://www.ftc.gov/ogc/coppa1.pdf)

Regulations -- 16 CFR Part 312 available at http://www.ftc.gov/os/1999/10/64fr59888.pdf (http://www.ftc.gov/os/1999/10/64fr9888.pdf)

"Personal information" means individually identifiable information about an individual collected online. [16 CFR 312.2]

Data Field Examples - Categories of Personal Information: first and last name; home or other physical address including street name and name of a city or town; an email address or other online contact information; including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's email address; telephone number; Social Security Numbers; a persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information, or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

FERPA educational institution student privacy regulation

The Family Educational Rights and Privacy is a US Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Express policy for FERPA (Family Educational Rights and Privacy Act), applied to educational institutions in the US.

Canadian Personal Information Protection and Electronic

Documents Act PIPEDA

The Personal Information Protection and Electronic Documents Act is a Canadian law governing how private sector organizations collect, use and disclose personal information in the course of commercial business. Canadian privacy law against identity theft.

Check 21 Act

The Check Clearing for the 21st Century Act (Check 21) is a Federal law designed to foster innovation in the payments system and to enhance its efficiency by reducing some of the legal impediments to check truncation.

Policy to be applied on scanned check files in TIFF format, according to the Check Clearing for the 21st Century Act (Check 21).

FFIEC

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the Federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions

Payment Card Industry (PCI)

The Payment Card Industry (PCI) Data Security Standard (PCI DSS, derived from Visa CISP) is a common industry standard that is accepted internationally by all major credit card issuers. The standard is enforced on companies that accept credit card payments, as well as other companies and organization that process, store, or transmit cardholder data.

Payment card industry rules for credit card data protection. Can be used in conjunction with GLBA and/or HIPAA policies for private customer data (such as SSN).

US Securities and Exchange Commission (SEC)

Policies for detection of SEC forms 10-K and 10-Q, based on calendar fiscal year.

Sarbanes-Oxley Financial and Accounting Disclosure Information (SOX)

The Sarbanes-Oxley Act (SOX) mandates public companies to comply with its requirements. This act provides strict guidelines for ensuring corporate governance and control policies for information within publicly traded companies. Websense Data

Security SOX related policies for Information Leak Prevention perspective are based on SOX audit terms and detection of SEC 10-K and 10-Q reports.

FISMA

The Federal Information Security Management Act of 2002 (FISMA) aims to reinforce computer and network security within the Federal Government and affiliated parties (such as government contractors). The type of information that should be protected depends on the relevant agency/sector.

DIACAP

The DoD Information Assurance Certification and Accreditation Process (DIACAP) is the US Department of Defense process to ensure the management of risks on Information Systems (IS). The policy is applied to information systems of DoD-related units and contractors. The DLP aspect of the policy applies to combinations of Personally Identifiable Information (like social security number or credit card number) with sensitive private information, such as health conditions, names of crimes, and ethnicities, to promote compliance with DoD Privacy Program (DoD 5400.11-R) and Privacy of Health Information in DoD Health Care (DoD 6025.18). Additional rules detect confidential information about the corporate network, and confidential documents, according to DoD 8520.1 - Protection of Sensitive Compartmented Information (SCI).

FDA - 21 CFR

Title 21 Part 11 of the Code of Federal Regulations (CFR) deals with the FDA guidelines on electronic records and electronic signatures in the United States. Part 11 requires drug makers, medical device manufacturers, biotech companies, biologics developers, and other FDA-regulated industries, with some specific exceptions, to implement controls, including audits, system validations, audit trails, electronic signatures, and documentation for software and systems involved in processing electronic data that are (a) required to be maintained by the FDA predicate rules or (b) used to demonstrate compliance to a predicate rule.

FCRA

The Fair Credit Reporting Act's primary protection requires that CRAs follow "reasonable procedures" to protect the confidentiality, accuracy, and relevance of credit information.

MITS

The Management of Information Technology Security (MITS) standard defines baseline security requirements that Canadian federal departments must fulfill to ensure the security of information and information technology (IT) assets under their control. The DLP aspect of the policy applies to combinations of Personally Identifiable Information (like social insurance number or credit card number) with sensitive private information, such as health conditions, to promote compliance with the Canadian Privacy Impact Assessment mandated by MITS. Additional rules detect confidential information about the corporate network, and confidential documents, to promote compliance with the Canadian Government Security Policy.

ITAR

The ITAR regulation for industry and government regulates dissemination of encryption, space, military and nuclear technology, along with source code.

FERC

The Federal Regulations and Oversight of Energy regulations (FERC) protects Critical Energy Infrastructure Information (CEII). The policy detects sensitive Energy Infrastructure Information, such as natural gas pipeline flow diagrams.

NYSE Rule 472

NYSE Rule 472 regulates communications with investors and mandates approval of communications and research reports before being released as well as the retention and archiving of such communications.

United States - State Laws

The following predefined policies can be applied in accordance with state-wide privacy regulations, as follows:

- *Arizona*, page 326
- *California*, page 326
- *Colorado*, page 327
- *Connecticut*, page 327
- *Delaware*, page 327
- *District of Columbia*, page 327
- *Florida*, page 328
- *Georgia*, page 328
- *Illinois*, page 328
- *Indiana*, page 328
- *Iowa*, page 328
- *Massachusetts*, page 328
- *Michigan*, page 328
- *Minnesota*, page 329
- *Nevada*, page 329
- *New Jersey*, page 329
- *New York State*, page 329
- *North Carolina*, page 329

Arizona

Arizona SB 1338 (http://www.azleg.gov/legtext/47leg/2r/bills/sb1338h.pdf (http://www.azleg.gov/legtext/47leg/2r/bills/sb1338h.pdf))

Requires a person who conducts business in Arizona and owns or licenses unencrypted computerized data that includes personal information to maintain its secrecy and confidentiality and to report about incidents that materially compromises the security or confidentiality of personal information.

Arkansas

Arkansas SB 1167 requires organizations to protect personal information of Arkansas residents (including personal health information) and to inform Arkansas customers when their private information is disclosed during a security breach. The policy comprises rules that detect combinations of personally identifiable information combinations with sensitive information such as private health information, credit card numbers, or passwords.

California

California AB 1950: requires organizations to notify Californians if their personal information is disclosed during a security breach. This law adds medical information to the information to be protected and extended the responsibility to organizations outside of the State, if they collect information about California residents. It does not apply to organizations that are subject to other privacy laws.

"Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional. [1798.81.5(d)]

California SB 1386: requires organizations to notify Californians if their personal information is disclosed during a security breach. SB 1386 is directed at state agencies and businesses operating in California. Personal information is defined as an individual's first name or first initial and last name with any of the following.

- Social Security number
- Driver's license number or California Identification Card number, or
- Account number, credit or debit card number, in combination with something like a PIN or password which would allow access to the account.

SB1: California Financial Information Privacy Act (also known as SB 1) requires financial institutions to provide their consumers notice and meaningful choice about how consumers' nonpublic personal information is shared or sold by their financial institutions. It provides greater privacy protections than those provided by the Gramm-Leach-Bliley Act.

California AB 1298: requires organizations to protect Californians' personal information (including personal health information) and to inform Californians when their private information is disclosed during a security breach. The policy comprises rules that detect combinations of personally identifiable information combinations with sensitive information such as private health information, credit card numbers, or passwords.

California SB 541 and AB 211: these amend the California Health and Safety Code and section 56.36 of the Civil Code. The bills give the state of California the ability to assess and enforce high fines for unauthorized leakage or access of private health information and create a new State Office of Health Information Integrity (OHII) to oversee data issues. The policy detects combinations of Personally Identifiable Information (PII) like names, social security or credit card number, and sensitive health information such as medical condition and DNA profiles.

Colorado

Colorado HB 1119 requires any individual or commercial entity that conducts business in Colorado and owns or licenses computerized data that includes Private Information or maintains such data to provide consumer notification of data breaches. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and Colorado driver license numbers.

Connecticut

State Privacy Laws SB 650 using names as identifiers. Searches for combinations of names Social Security numbers, credit card numbers, drivers' license or password.

Delaware

State Privacy Laws HB 116 using names as identifiers. Searches for combinations of names Social Security numbers, credit card numbers, drivers' license or password.

District of Columbia

District of Columbia 28-3852 mandates that consumers should be notified when electronically-stored personal information is compromised in a way that increases the risk of identity theft. The policy detects unencrypted combinations of Personally Identifiable Information (PII) like full names, social security numbers, DC driver license and credit card numbers. Additional rules detect passwords.

Florida

Florida HB 481 requires businesses maintaining computerized data including PI to provide notice of security system breach in certain circumstances. This State law affects any person that conducts business in Florida and owns or licenses computerized data that includes PI or maintains such data.

Georgia

Georgia SB 230 requires expeditious notification of unauthorized acquisition and possible misuse of PI. This State policy applies to information brokers that own or license computerized data that includes PI or a person or business who maintains such data on behalf of brokers.

Illinois

Illinois HB 163 requires data collector to provide notification of security breach after discovery, even if data has not been accessed by unauthorized person. This State law affects all data collectors that own or license PI or maintains computerized data that includes PI.

Indiana

State Privacy Laws SB 503 using names as identifiers. Searches for combinations of names Social Security numbers, credit card numbers, drivers' license or password.

Iowa

Iowa SF 2308 requires notification of Iowa consumers of a security breach involving personal information by the person who owns, maintains or otherwise possesses the information. The policy detects unencrypted combinations of Personally Identifiable Information (PII) like full names, social security numbers, DNA data, Iowa driver license and credit card numbers. Additional rules detect passwords.

Massachusetts

Massachusetts 201 CMR 17 mandates that a business in Massachusetts shall encrypt any personal information of a customer that is transmitted over public networks or stored on laptops or removable memory. The policy detects unencrypted combinations of Personally Identifiable Information (PII) like full names, social security numbers, Massachusetts driver license and credit card numbers. Additional rules detect passwords.

Michigan

Michigan Privacy Act SB 309 requires a state agency or a private company that maintains computerized data with personalized information on individuals to notify those individuals if a breach of security allows unencrypted personal identifying information to be acquired by an unauthorized person. Failure to comply with the notification requirements would be punishable by civil fines up to a maximum of $2.5 million. The policy detects combinations of Personally Identifiable Information (PII) like social security numbers, Michigan driver license, credit card numbers, and DNA.

Minnesota

Minnesota Code 325E.61 requires businesses to provide consumer notification of data breaches. It is applicable to any person that conducts business in Minnesota and owns or licenses computerized data that includes PI or maintains such data. The policy detects combinations of Personally Identifiable Information (PII) like Social Security, credit card, and Minnesota driver license numbers.

Contains two rules:

- Social Security Number with Minnesota Driver license
- Social Security Number with Credit Card Number

Nevada

Nevada NRS 597.970 mandates that a business in Nevada shall not transfer electronically any personal information of a customer to a person outside of the secure system of the business unless encryption is used. The policy detects Personally Identifiable Information (PII) that should be encrypted, like full names with social security numbers, Nevada driver license, credit card numbers, and passwords.

New Jersey

New Jersey A 4001 requires business or public entity that are compiling or maintaining computerized data with PI to disclose security breach if PI is reasonably believed to be acquired by unauthorized person. This State law affects any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that includes PI or any business or public entity that compiles or maintains such records.

New York State

New York AB 4254 Guarantees persons the right to know what information was exposed during a breach, so that they can take the necessary steps to both prevent and repair any damage incurred.

North Carolina

North Carolina Identity Theft Protection Act, SB 1048, mandates protection of personal information and requires NC businesses to notify consumers in case of a security breach. The policy detects unencrypted combinations of Personally Identifiable Information (PII) like full names with social security numbers, NC driver licenses, and credit card numbers.

Ohio

Ohio HB 104 mandates that consumers should be notified when electronically-stored personal information is compromised in a way that increases the risk of identity theft. The policy detects unencrypted combinations of Personally Identifiable Information (PII) like full names, social security numbers, Ohio driver licenses, and credit card numbers. Additional rules detect passwords.

Pennsylvania

State Privacy Laws SB 712 using names as identifiers. Searches for combinations of names Social Security numbers, credit card numbers, drivers' license or password.

Texas

Texas SB 122 requires that any person who conducts business in Texas and owns or licenses computerized data that includes sensitive Private Information will take reasonable measures to protect the information.

Utah

S.B. 69

3/20/06 Signed by Governor, Chapter 343

Requires a person maintaining personal information in connection with a business to implement procedures to protect personal information; requires destruction of certain records; requires disclosure of breaches of databases containing personal information; and provides for enforcement by the attorney general.

Virginia

Virginia SB 307 mandates that consumers should be notified when their personal information is compromised in a way that increases the risk of identity theft or other fraud. The bill also requires covered entities to notify the state attorney general in the case of breaches of personal information of more than 1,000 residents. The policy detects unencrypted combinations of Personally Identifiable Information (PII) like full names, social security numbers, Virginia driver license and credit card numbers.

Washington

The Security of Personal Information Senate Bill 6043 requires any person or business that owns or licenses computerized data that includes PI must disclose security system breach to those whose unencrypted PI was/is reasonably believed to be acquired by an unauthorized person.

Wisconsin

03/16/06 Signed by Governor, Act 138

Requires an entity that possesses certain personal information about an individual to notify the individual when the information is accessed by a person who the individual has not authorized to do so (unauthorized access). The bill's notice requirements apply to entities, including the state and local governments, that do any of the following: conduct business in Wisconsin and maintain personal information in the ordinary course of business; store personal information in this state; maintain a depository account for a Wisconsin resident; or lend money to a Wisconsin resident (from http://www.ncsl.org/programs/lis/cip/priv/breach06.htm#wisconsin (http://www.ncsl.org/programs/lis/cip/priv/breach06.htm#wisconsin)).

EMEA Policies

The EMEA policies detect the following:

- *EU*, page 331
- *Denmark*, page 332
- *Finland*, page 332
- *France*, page 332
- *Germany*, page 332
- *Greece*, page 332
- *Iceland*, page 332
- *Ireland*, page 333
- *Israel*, page 333
- *Italy*, page 333
- *Netherlands*, page 333
- *Norway*, page 333
- *Poland*, page 334
- *Russia*, page 334
- *South Africa*, page 334
- *Spain*, page 334
- *Sweden*, page 334
- *Switzerland*, page 335
- *Turkey*, page 335
- *United Kingdom*, page 335

EU

Directive 95/46/EC on the protection of personal data regulates the processing of personal data, regardless if the processing is automated or not.

Also, the EU finance policy promotes regulatory compliance with the requirements of the Basel Committee on Banking Supervision. The policy contains rules to detect financial data like account numbers, passwords, or magnetic credit card tracks.

Additional rules detect combinations of Personally Identifiable Information (PII) like credit cards and identification numbers.

Denmark

The Denmark Personal Information Protection Law (PIP) regulates the handling of personal information. The policy comprises rules for detection of CPR numbers and Danish bank account numbers.

Finland

Finland's Personal Data Act provides restrictions on the processing, storage and transmission of personal and sensitive information, including personal ID. Under the Law, personal information relating to identity may only be processed, stored and transmitted with the consent of the individual. Personal information cannot generally be transferred outside of Finland unless the country has 'comparable' protections. The policy comprises rules for detection of Finnish Social Security Numbers and DNA sequences.

France

Policy for the French Law 2004-801, which implements the EU Directive 95 on privacy. The policy contains rules to detect combinations of French full names and INSEE numbers with sensitive private information like credit card number or health conditions.

Germany

The German Federal Privacy Protection Act (Bundesdatenschutzgesetz) implements the Directive 95/46/EC on the protection of personal data. It regulates the s that can taken on personal data: storage, deletion, transfer, and others. It defines the rights of individuals with regards to their data entitled to protection: notification, correction, etc. In case of improper s on the data, it distinguishes between criminal and administrative violations and provides right to damages. Full text (in English): http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg01_eng.htm.

Greece

The Hellenic Data Protection Act of 1997 regulates the processing of personal data and therefore mandates the protection of private information. The policy detects Greek AFM and ID numbers, alone or in proximity to a Greek names in Greek or Latin letters, and combinations of Greek names in proximity to sensitive medical information in Greek and English.

Iceland

The Iceland Act on Protection of Individuals with regard to the Processing of Personal Information (law 77/2000) follows the EU Data Protection Directive and restricts the processing, storage and transmission of personal and sensitive information. The predefined policy comprises rules for detection of Iceland identification numbers (kennitala) and DNA profile.

Ireland

The Irish Data Protection (Amendment) Act of 2003 provides provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use, or disclosure of such information. The policy contains rules to detect Irish Personally Identifiable Information (PII) like Personal Public Service Numbers (PPS) or passport numbers, alone or in combination with credit card numbers.

Israel

Policy for detection of private health information of Israeli citizens, to promote compliance with Israeli privacy rules and Israeli patients rights law of 1996.

Policy to cover the Israeli NBT directive, which requires Israeli banks and agencies to protect customers privacy by ensuring the integrity and confidentiality of data. The policy detects credit card information, account numbers, International Bank accounts number (Israeli IBAN) and buy and sell instructions in Hebrew.

Italy

The Italy Health Data Privacy Act protects persons from violation of their right to privacy through the processing of personal data. The Act helps to ensure that personal data is processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensures that personal data is of adequate quality. The policy contains rules to detect combinations of Italy Personally Identifiable Information (PII) like Codice Fiscale and full name, with sensitive health information.

Netherlands

Policy to promote compliance with the Dutch Personal Data Protection Act, which implements the EU Directive 95 on privacy. The policy contains rules to detect combinations of Netherlands sofinummer and sensitive private information like account number, ethnicity and health conditions.

Norway

The Norway Health Data Privacy Act protects persons from violation of their right to privacy through the processing of personal data. The Act helps to ensure that personal data is processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensures that personal data is of adequate quality. The policy contains rules to detect combinations of Norwegian Personally Identifiable Information (PII) like personnummer and full name, with sensitive health information.

Poland

The Law on the Protection of Personal Data (LPPD) is based on the European Union (EU) Data Protection Directive. Under the law, personal information relating to identity may only be processed, stored and transmitted with the consent of the individual. Personal information cannot generally be transferred outside of Poland unless the country has 'comparable' protections. The law sets out civil and criminal sanctions for violations. The policy comprises rules for detection of Polish NIP numbers, PESEL numbers, Polish ID numbers, DNA information and Polish REGON numbers, alone or in proximity to a Polish name.

Russia

The law of the Russian Federation on Information, Informatization, and Information Protection of 1995 covers both the government and private sectors and imposes a code of fair information practices and other restrictions on the processing of personal and sensitive information. The pre-defined policy comprises rules for detection of a Russian passport number when appearing together with Russian full names and for detection of DNA information.

South Africa

The Republic of South Africa Electronic Communication and Transaction Act defines a national e-strategy for the Republic and also prevent abuse of information systems to encourage the use of e-government services and to provide for matters connected therewith. Chapter VIII of the act deals with protection of personal information. The policy detects combinations of valid South Africa ID number with credit card numbers.

Spain

Organic Law 15/1999 on the Protection of Personal Data (LOPD) implemented Directive 95/46/EC into Spanish law. The law establishes the right of citizens to know what personal data is contained in computer files and the right to correct or delete incorrect or false data. Personal information may only be used or disclosed to a third party with the consent of the individual and only for the purpose for which it was collected. Additional protections are provided for sensitive data. Source: http://www.privacyinternational.org/survey/phr2003/countries/spain.htm

Sweden

Sweden's Personal Data Act of 1998 was enacted to protect people against the violation of their personal integrity by processing of personal data. The act includes restrictions on the storage and transmission of personal data. The pre-defined policy comprises rules for detection of Swedish Personal Identity Number (personnummer) in traffic and DNA information.

Switzerland

The Federal Act of Data Protection of 1992 regulates personal information held by government and private bodies. The Act requires that information must be legally and fairly collected and places limits on its use and disclosure to third parties. Transfers to other nations must be registered and the recipient nation must have equivalent laws. The pre-defined policy comprises rules for detection of Swiss AHV numbers and DNA information.

Turkey

A policy for protection of personal information, in accordance with Turkey's "Protection of Personal Data" Draft Law.

United Kingdom

The UK Data Protection Act 1998 provides provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The act defines eight principles of information-handling practice, concerning the security measures and permissions that need to be taken with regards to private and sensitive information. The data that is covered by the act includes personally identifiable information such as identification numbers (National Insurance Numbers, Driver Numbers, etc), birth dates, addresses and similar data held on computers.

APAC Regulations

Predefined policies can detect traffic in accordance with the following APAC Regulations:

- *Australia*, page 335
- *Hong Kong*, page 336
- *Japan*, page 336
- *New Zealand*, page 336
- *Singapore*, page 336
- *Taiwan*, page 336
- *Thailand*, page 336

Australia

The Australian Federal Privacy Act is very broad and contains eleven Information Privacy Principles which apply to government agencies. It also has ten National Privacy Principles which apply to parts of the private sector and all health service providers. It also regulates credit providers and credit reporting agencies.

Hong Kong

The Hong Kong Personal Data Privacy Ordinance (PDPO) protects the privacy interests of living individuals in relation to personal data. The Ordinance covers any data relating directly or indirectly to a living individual from which it is practicable to ascertain the identity of the individual and which are in a form in which access or processing is practicable, including, for example, Hong Kong Identity Card Number, name and address.

Japan

The Japan Personal Information Protection Law (PIP) states a set of obligations for companies handling personal data. The law protects individuals by regulating the handling of information by private sector businesses. The policy contains rules to protect Japan PII (Personally Identifiable Information), either alone or with a credit card number.

New Zealand

New Zealand's Privacy Act of 1993 applies to almost every person, business or organization in New Zealand. The act sets out information privacy principles, which, among others, limit transmission and storage of personal data. The pre-defined policy comprises rules for detection and monitoring of NZ National Health Index (NHI) numbers and DNA information.

Singapore

The Singapore Electronic Transaction Act (ETA) mandates applying adequate measures to assure the confidentiality of electronic records, imposing fines and incarceration for compromising confidentiality. It also outlines the liability of directors, managers, secretaries and other officers of the body corporate in case of a breach.

Taiwan

Policy containing rules to protect Taiwanese personal information in line with the Taiwan Personal Information Protection Act.

Thailand

The Thailand Official Information Act, B.E. 2540 of 1997 sets a code of information practices for the processing of personal information by state agencies. The act mandates, among other things, not to disclose personal information to other state agencies or other persons without prior consent given in writing, except in limited circumstances. The pre-defined policy comprises rules for detecting validated Thai National ID Numbers and DNA sequences.

- Suspected Passwords
- Credit Card Tracks (contents of the magnetic strips)

- Social Security Numbers (NLP, ITIN)
- Credit Card Numbers (NLP)

Data Discovery policies

The predefined data discovery policies are categorized as follows:

- PCI
- Private Information
- Company Confidential and Intellectual Property
- Acceptable Use
- Regulations

PCI

For information on the PCI standard, see *Payment Card Industry (PCI)*, page 323.

Private Information

Predefined discovery policies are available to detect personally identifiable information for the following countries:

- Sweden
- Ireland
- Switzerland
- France
- Russia
- Denmark
- Germany
- Iceland
- Israel
- Italy
- Japan
- Netherlands
- Norway
- Brazil
- Mexico
- Australia
- Singapore
- Hong Kong

- Macau
- Malaysia
- South Korea
- Taiwan
- People’s Republic of China
- New Zealand
- United States and Canada
- Poland
- South Africa
- Spain
- Turkey
- United Kingdom

Discovery policies are also available to detect the following:

- Credit card numbers
- Social security numbers
- General sensitive information, whose loss may damage the privacy or the reputation of the pertained person or expose the person to potential fraud. This policy comprises rules for detection of various kinds of sensitive private information, such as private health information, account numbers, and passwords.

Company Confidential and Intellectual Property

The following discovery policies are available for company confidential and intellectual property information:

- Call Detail Records
- Document Properties
- Strategic planning documents
- Network Security Information
- Patents
- Petroleum and Gas Sensitive Information
- Software Design Documents
- Software Source Code
- Movie Manuscripts
- Hardware Source Code
- Financial Information
- Mergers and Acquisitions
- Pricing Information

Acceptable Use

The following discovery policies are available for acceptable use policy tracking:

- Acceptable Usage - Obscenities & Racism
- W-2 Forms
- Resumes: policies for detection in English, Hebrew, Russian and Ukrainian
- Email Addresses
- License Keys

Regulations

The following discovery policies are available for regulations:

- FERC. For more information, see *FERC*, page 325.
- SEC and SOX. For more information, see *US Securities and Exchange Commission (SEC)*, page 323, and *Sarbanes-Oxley Financial and Accounting Disclosure Information (SOX)*, page 323.
- ITAR. For more information, see *ITAR*, page 325.

B Predefined Classifiers

This appendix provides a list of all the predefined content classifiers that Websense Data Security provides for detecting events and threats involving secured data. This includes:

- *File-type classifiers*
- *NLP scripts*
- *Dictionaries*
- *PreciseID patterns*

The classifiers are constantly being updated and added to. To get the most up-to-date classifiers:

1. On the Main tab, go to Data Usage Policies or Data Discovery Policies.
2. Click **Policy Templates** on the toolbar.
3. On the Policy Templates page, click **Install Updates.**
4. Proceed through the update wizard. This updates your predefined policies and content classifiers.

File-type classifiers

This section contains the full list of file-type classifiers provided by Websense.

Classifier	Description
SmartWare II Database File	Detection of SmartWare II Database files according to internal file properties.
MS Works Database File (for Macintosh)	Detection of MS Works Database files for Macintosh according to internal file properties.
MS Works Database File (for DOS)	Detection of MS Works Database files for DOS according to internal file properties.
MS Works Database File (for Windows)	Detection of MS Works Database files for Windows according to internal file properties.
Paradox Database File	Detection of Paradox Database files according to internal file properties.

Classifier	Description
AutoCAD DFX Binary File	Detection of Autodesk DXF binary file format according to internal file properties.
AutoCAD DFX Text File	Detection of Autodesk DXF textual file format according to internal file properties.
dBase File	Detection of dBase Database file format according to internal file properties.
Ability DataBase File	Detection of Ability Office DataBase file format according to internal file properties.
PGP Encrypted File	Detection of encrypted PGP file format according to internal file properties.
PGP Signed and Encrypted File	Detection of signed and encrypted PGP file format according to internal file properties.
Autodesk DWG File	Detection of Autodesk DWG CAD file format according to internal file properties.
Autodesk WHIP File	Detection of Autodesk Whip file format according to internal file properties.
Microsoft Access File	Detection of MS Access Database files according to internal file properties.
Microsoft Access File (All Versions)	Detection of MS Access Database files (all versions) according to internal file properties.
Microsoft Access 2000 File	Detection of MS Access 2000 Database files according to internal file properties.
Microsoft Access 95 File	Detection of MS Access 95 Database files according to internal file properties.
Microsoft Access 97 File	Detection of MS Access 97 Database files according to internal file properties.
Microsoft Visio File	Detection of MS Visio files according to internal file properties.
Microsdt Visio XML File	Detection of MS Visio XML files according to internal file properties.
Lotus Notes NSF File	Detection of IBM Lotus Notes Database NSF/NTF files according to internal file properties.
MORE Database File	Detection of MORE Database files for Macintosh according to internal file properties.
CATIA File	Detection of CATIA file format according to internal file properties.
Encrypted ZIP File	Detection of encrypted ZIP archives according to internal file properties.
Encrypted Excel File	Detection of encrypted Microsoft Excel file format according to internal file properties.
Encrypted Word File	Detection of encrypted Microsoft Word file format according to internal file properties.
Encrypted PDF File	Detection of encrypted PDF documents according to internal file properties.

Classifier	Description
Encrypted RAR File	Detection of encrypted RAR archives according to internal file properties.
FileMaker File	Detection of Filemaker Database files for Macintosh according to internal file properties.
Corel Draw File	Detection of CorelDRAW file format according to internal file properties.
Microsoft Excel File - All Versions	Detection of MS Excel files (all versions) according to internal file properties.
Microsoft Visio File - All Versions	Detection of MS Visio files (all versions) according to internal file properties.
Microsoft Word File - All Versions	Detection of MS Word files (all versions) according to internal file properties.
Portable Document Format (PDF) - All Versions	Detection of PDF files according to internal properties.
Tagged Image File Format (TIFF) File	Detection of TIFF (Tagged Image File Format) files according to internal properties.
Various Archive Formats	Detection of 7-zip, BinHex, GZIP, Legato EMailXtender Archive, MS CAB, ZIP archive format, RAR format, UNIX TAR encapsulation.
Various Executables Formats	Detection of Windows Executable files, Link Libraries, MS Com executables.
Various Computer Aided Design Formats	Detection of AutoCAD DXF graphics, AutoCAD Drawing, CATIA formats, MS Visio, MicroStation.
Various DataBase Formats	Detection of MS Access, MS Project.
Various Graphics Formats	Detection of Computer Graphics Metafile, CorelDRAW, DCX Fax System, Encapsulated PostScript, Enhanced Metafile, GIF, JPEG, Lotus AMIDraw Graphics, Lotus Pic, MacPaint, MS Office Drawing, PC PaintBrush, Portable Network Graphics, SGI RGB Image, Sun Raster Image, Tagged Image File, Truevision Targa, Windows Animated Cursor, Windows Bitmap, Windows Icon Cursor, Windows Metafile, Word Perfect Graphics.
Various Mail Formats	Detection of Domino XML, Legato Extender, Lotus Notes DB, MS Outlook, MS Outlook Express, MS Outlook Personal Folder, Text Mail (MIME), Transport Neutral Encapsulation Format.
Various MultiMedia Formats	Detection of Advanced Streaming Format (ASF), Audio Interchage File Format (AIFF), MS Wave Sound (WAV), MIDI, MP3, Mpeg-1 Video, Mpeg-2 Audio, NeXT/Sun Audio, Quick Time Movie, Windows Video (AVI).
Various Presentation Formats	Detection of MS PowerPoint, Apple iWork Keynote, Corel Presentations, Lotus Freelance Graphics 2, Macromedia Flash, Applix Graphics, Star Office Impress.

Classifier	Description
Various Spreadsheet Formats	Detection of MS Excel, Apple iWork Numbers, Applix Spreadsheets, Comma Separated Values (CSV), Data Interchange Format, Lotus 1-2-3, MS Works Spreadsheet, Star Office Spreadsheet.
Various Text and Markup Formats	Detection of ASCII, HTML, MS Excel Windows XML, MS Word Windows XML, MS Visio XML, MIME HTML, Rich Text Format (RTF), Unicode Text, XHTML, XML.
Various Word Processing Formats	Detection of MS Word, Adobe FrameMaker Interchange, Apple iWork Pages, Applix Words, Corel WordPerfect, Display Write, Folio Flat File, Founder Chinese E-Paper Basic, Oasys, Haansoft Hangul, IBM DCA/RFT, Just Systems Ichitaro, Lotus AMI, Lotus Word, MS Works, Star Office Writer, WordPad, XML Paper Specification, XyWrite, Yahoo Instant Messenger.
Solid Works File	Detection of SolidWorks files.

NLP scripts

This section contains the full list of natural language processing scripts provided by Websense.

Classifier	Description
Iceland SSN (Default)	Detection of Iceland identification numbers (kennitala), employing various heuristics involving kennitala-related terms and other features unique to this number
Iceland SSN (Wide)	Detection of Iceland identification numbers (kennitala), employing various heuristics involving features unique to this number
W2 Form Support	Detection of IRS W2 forms
CV in English	Detection of CV in English, using location-sensitive lexical analysis of terms and patterns common in such documents
CV in Russian or Ukranian	Detection of CV in Russian or Ukranian, using location-sensitive lexical analysis of terms and patterns common in such documents
Source code: Verilog	Detection of Verilog source code, using lexical analysis of terms, patterns, and structures for optimal accuracy
Source code: C or JAVA	Detection of source code content written in C, C++, C# or Java, using lexical analysis of terms, patterns, and structures for optimal accuracy
Source code: C or JAVA (Wide)	Detection of files which are suspected to be source code content - written in C, C++, C# or Java, using lexical analysis of terms, patterns and structures.
Email Addresses	Detection of email addresses
Email Addresses Domains	Detection of email addresses having different domains

Classifier	Description
MAC Address (Wide)	Detection of MAC addresses. Detects delimited MAC addresses and non-delimited MAC addresses with support terms in proximity
MAC Address (Default)	Detection of MAC addresses; detects only delimited MAC addresses
MAC Address (Narrow)	Detection of MAC addresses; detects delimited MAC addresses with a valid OUI (Organizationally Unique Identifier)
Filter - Source Code	Optimization filter for fast detection of probable source code data.
CCN - for printer agent	Detection of valid credit card numbers, employing context-sensitive lexical analysis and statistical analysis of patterns, taking into account possible errors that may be induced by the OCR software
Latitude-Longitude coordinates	Detection of latitude-longitude coordinates
Routing Number (Wide)	Detection of issued RTNs
Routing Number (Default)	Detection of issued RTNs; includes advanced statistical heuristics
Routing Number (Narrow)	Detection of issued RTNs; includes advanced statistical heuristics and search for support terms
IMEI (Wide)	Detection of validated IMEI numbers, delimited and non-delimited
IMEI (Default)	Detection of validated IMEI numbers, delimited and non-delimited. Also locates IMEI-related term somewhere in the document
Russian Passport	Detection of Russian passport numbers
Russian Names (Wide)	Detection of Russian full names
Russian Names (Default)	Detection of Russian full names
Russian Names (Narrow)	Detection of Russian full names
Malicious Concealment	Detection of content suspected to be manipulated (for example, by replacing letters with symbols) to avoid detection, using methods such as statistical analysis
Text in Header/Footer	Detection of any user-defined term in the header or footer of documents
10K Form	Detection of 10K forms
10K Form (Non Standard Fiscal Year)	Detection of 10K forms for non-standard fiscal years (not ending at 31/12)
10Q Form	Detection of 10Q forms
10Q Form (Non Standard Fiscal Year)	Detection of 10Q forms for non-standard fiscal years (not ending at 31/12)

Classifier	Description
CDR	Detection of Call Detail Records with information like source phone number, destination phone number, call date, duration, etc.
CDR: headers	Detection of Call Detail Records by looking for column headers related to information such as source phone number, destination phone number, call date, duration, etc.
Israeli Credit Cards (Default)	Detection of Israeli credit card numbers (not including Isracard) employing various heuristics involving credit card related terms and use of delimiters. By default, only the first 4 digits and the last 4 digits are shown in the reports.
Israeli Credit Cards (Wide)	Detection of potential Israeli credit card numbers (not including Isracard), based only on format and validation, may cause false positives. By default, only the first 4 digits and the last 4 digits are shown in the reports.
Israeli Credit Cards (Narrow)	Detection of Israeli credit card numbers (not including Isracard). Requires additional evidence, such as credit card related terms in proximity, in order to qualify number as a credit card number. By default, only the first 4 digits and the last 4 digits are shown in the reports.
US Credit Cards (Default)	Detection of credit card numbers employing various heuristics involving credit-card related terms and use of delimiters. By default, only the first 4 digits and the last 4 digits are shown in the reports
US Credit Cards (Wide)	Detection of potential credit card numbers, based only on format and validation; may cause false-positives. By default, only the first 4 digits and the last 4 digits are shown in the reports
US Credit Cards (Narrow)	Detection of credit card numbers; requires additional evidence, such as credit-card related terms in proximity, in order to qualify number as a credit-card number. By default, only the first 4 digits and the last 4 digits are shown in the reports
EU Credit Cards	Detection of valid credit card numbers prevalent in Europe, employing various heuristics involving credit-card related terms and use of delimiters
South Africa ID	Detection of valid South Africa ID numbers
Japanese Credit Cards	Detection of valid credit card numbers prevalent in Japan, employing various heuristics involving credit-card related terms and use of delimiters. The terms and credit card digits are detected in both English and Japanese
Israeli Credit Cards	Detection of valid credit card numbers prevalent in Israel
Turkey TC Kimlik	Detection of validated Turkish Citizenship numbers (TC Kimlik), when appearing in proximity to TC Kimlik-related terms in English, Turkish and other European languages
Turkey TC Kimlik: one support only	Detection of validated Turkish Citizenship numbers (TC Kimlik), when there is at least one related term appearing in the document

Classifier	Description
Turkey PII in Spreadsheets	Detection of spreadsheets containing Turkish personally identifiable information (PII) by looking for column headers related to information such as full name, address, citizenship number, etc.
IBAN Turkey	Detection of Turkish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Turkish IBAN format
IBAN Turkey (Wide)	Detection of Turkish IBANs (International Bank Account Numbers) without support terms in proximity
IBAN Germany	Detection of German IBANs (International Bank Account Numbers). Searches for support terms in proximity to German IBAN format
IBAN Germany (Wide)	Detection of German IBANs (International Bank Account Numbers) without support terms in proximity
German Names	Detection of German full names
IBAN Netherlands	Detection of Netherlands IBANs (International Bank Account Numbers). Searches for support terms in proximity to Netherlands IBAN format
IBAN Netherlands (Wide)	Detection of Netherlands IBANs (International Bank Account Numbers) without support terms in proximity
IBAN Switzerland	Detection of Swiss IBANs (International Bank Account Numbers). Searches for support terms in proximity to Swiss IBAN format
IBAN Switzerland (Wide)	Detection of Swiss IBANs (International Bank Account Numbers) without support terms in proximity
IBAN Norway	Detection of Norwegian IBANs (International Bank Account Numbers). Searches for support terms in proximity to Norwegian IBAN format
IBAN Norway (Wide)	Detection of Norwegian IBANs (International Bank Account Numbers) without support terms in proximity
Norway Personnummer	Detection of Norway Personal Numbers (personnummer), possibly in proximity to related terms
Norwegian Names	Detection of Norwegian full names
IBAN Italy	Detection of Italian IBANs (International Bank Account Numbers). Searches for support terms in proximity to Italian IBAN format
IBAN Italy (Wide)	Detection of Italian IBANs (International Bank Account Numbers) without support terms in proximity
Italy Codice Fiscale Number	Detection of validated Italy Codice Fiscale, possibly in proximity to related terms
Italian Names	Detection of Italian full names
IBAN Iceland	Detection of Icelandic IBANs (International Bank Account Numbers). Searches for support terms in proximity to Icelandic IBAN format

Classifier	Description
IBAN Iceland (Wide)	Detection of Icelandic IBANs (International Bank Account Numbers) without support terms in proximity
French Names	Detection of French full names
French INSEE Number	Detection of valid INSEE (NIR) numbers, validated with or without check digits
IBAN France	Detection of French IBANs (International Bank Account Numbers). Searches for support terms in proximity to French IBAN format
IBAN France (Wide)	Detection of French IBANs (International Bank Account Numbers) without support terms in proximity
IBAN Sweden	Detection of Swedish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Swedish IBAN format.
IBAN Sweden (Wide)	Detection of Swedish IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Finland	Detection of Finnish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Finnish IBAN format.
IBAN Finland (Wide)	Detection of Finnish IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Greece	Detection of Greek IBANs (International Bank Account Numbers). Searches for support terms in proximity to Greek IBAN format.
IBAN Greece (Wide)	Detection of Greek IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Denmark	Detection of Danish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Danish IBAN format.
IBAN Denmark (Wide)	Detection of Danish IBANs (International Bank Account Numbers) without support terms in proximity.
Poland: NIP Number	Detection of Polish NIP numbers
Poland: PESEL Number	Detection of Polish Pesel numbers
Poland: ID	Detection of Polish Identification numbers
Poland: REGON Number	Detection of REGON numbers
IBAN Poland	Detection of Polish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Polish IBAN format
IBAN Poland (Wide)	Detection of Polish IBANs (International Bank Account Numbers) without support terms in proximity
IBAN Ireland (Wide)	Detection of Irish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Irish IBAN format

Classifier	Description
IBAN Ireland	Detection of Irish IBANs (International Bank Account Numbers) without support terms in proximity
Irish Passport	Detection of Irish passport numbers
Ireland PPS	Detection of Irish Personal Public Service numbers
Ireland Account	Detection of Irish bank account numbers with support terms in proximity
Spain: DNI number	Detection of Spain DNIs, in proximity to related terms
Netherlands: Sofinummer	Detection of validated Netherlands Sofinummers, in proximity to related terms
1st Magnetic Track	Detection of the string encoded on the 1st magnetic track of a credit card, containing the card number, and personal information of the card holder
2nd Magnetic Track	Detection of the string encoded on the 2nd magnetic track of a credit card, containing the CCN, PIN, expiration date, and other card-issuer data
3rd Magnetic Track	Detection of the string encoded on the 3rd magnetic track of a credit card, containing the CCN, PIN, and other card-issuer data
US Passwords - keyboard sequence	Detection of passwords comprised of adjacent keyboard sequences.
PIN with proximity	Detection of PIN numbers in proximity to a PIN-related term
IBAN UK	Detection of UK IBANs (International Bank Account Numbers). Searches for support terms in proximity to UK IBAN format
IBAN UK (Wide)	Detection of UK IBANs (International Bank Account Numbers) without support terms in proximity
UK Driver Number	Detection of UK Driver Numbers
UK Voter Number	Detection of UK electoral roll numbers in proximity to related terms
IBAN Spain	Detection of Spanish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Spanish IBAN format
IBAN Spain (Wide)	Detection of Spanish IBANs (International Bank Account Numbers) without support terms in proximity
IL Bank accounts: Leumi	Detection of validated Leumi account numbers that include branch numbers, when appearing with terms relating to accounts in English or Hebrew
IL Bank accounts: Leumi no support	Detection of validated Leumi account numbers that include branch numbers
IL Bank accounts: Poalim	Detection of validated Poalim account numbers that include branch numbers, when appearing with terms relating to accounts in English or Hebrew

Classifier	Description
IL Bank accounts: Discount	Detection of validated Discount account numbers in proximity to terms related to accounts in English or Hebrew
IL Bank accounts: Mizrahi	Detection of validated Mizrahi account numbers that include branch numbers, when appearing with terms relating to accounts in English or Hebrew
IL Bank accounts: Benleumi	Detection of validated BenLeumi account numbers in proximity to terms related to accounts in English or Hebrew
IL Bank accounts: HaDoar	Detection of validated HaDoar account numbers, when appearing with terms relating to accounts in English or Hebrew
IL Generic Insurance Number - delimited	Detection of generic Israeli insurance policy numbers in standard delimitation.
IL Generic Insurance Number - nondelimited	Detection of generic Israeli insurance policy numbers without delimitation.
IL Life Insurance	Detection of Israeli life insurance numbers.
Israeli ID (Default)	Detection of valid Israeli Identification Numbers, employing context-sensitive lexical analysis, statistical analysis of patterns, and custom dictionaries
Israeli ID (Wide)	Permissive detection of valid Israeli Identification Numbers. Does not require support term in proximity
Israeli ID (Narrow)	Restricted detection of valid Israeli Identification Numbers; tune in order to minimize false-positives. Requires additional evidence, such as Israeli ID-related terms (English or Hebrew) in proximity
Israeli ID: 7 or 8 digits with proximity	Restricted detection of 7- or 8-digit valid Israeli Identification Numbers, when appearing in proximity to Israeli ID-related terms (English or Hebrew)
Israeli ID with proximity	Detection of Israeli ID numbers when appearing in proximity to Israeli ID related terms.
Israeli Life Insurance	Detection of Israeli life insurance numbers when appearing in proximity to life insurance related terms.
Israeli Insurance Claims	Detection of Israeli life insurance claims numbers when appearing in proximity to related terms.
Israeli IBAN	Detection of Israeli IBANs (International Bank Account Numbers). Searches for support terms in proximity to Israeli IBAN format
Israeli IBAN (Wide)	Detection of Israeli IBANs (International Bank Account Numbers) without support terms in proximity
US SSN (Wide)	Permissive detection of all delimitation forms of valid Social Security numbers that have been issued by the US Social Security Administration
US SSN (Default)	Detection of valid Social Security numbers that have been issued by the US Social Security Administration, employing context-sensitive lexical analysis, statistical analysis of patterns and custom dictionaries

Classifier	Description
US SSN (Narrow)	Restricted detection of valid Social Security numbers, which have been issued by the US Social Security Administration; tune in order to minimize false-positives. Requires additional evidence, such as SSN-related terms in proximity
US SSN: masked	Detection of valid social security numbers that have been issued by the US Social Security Administration, employing context sensitive lexical analysis, statistical analysis of patterns and custom dictionaries. By default, only the last 4 digits are shown in the reports.
US Names (Wide)	Detection of full names
US Names	Detection of full names
Driver License: Nevada	Detection of valid Nevada driver license number, in proximity to driver license terms, including typos and misspellings
Driver License: Massachusetts	Detection of valid Massachusetts driver license number, in proximity to driver license terms, including typos and misspellings
Driver License: Indiana	Detection of valid Indiana driver license number, in proximity to driver license terms, including typos and misspellings
Driver License: Utah	Detection of valid Utah driver license number, in proximity to driver license terms, including typos and misspellings
Driver License: Virginia	Detection of valid Virginia driver license number, in proximity to driver license terms, including typos and misspellings
Driver License: District of Columbia	Detection of valid District of Columbia driver license number, in proximity to driver license terms, including typos and misspellings
Driver License: Iowa	Detection of valid Iowa driver license number, in proximity to driver license terms, including typos and misspellings
SIN (Default)	Detection of valid Canadian social insurance numbers, employing context-sensitive lexical analysis, statistical analysis of patterns and custom dictionaries
SIN (Wide)	Permissive Detection of valid Canadian social insurance numbers. Does not require support term in proximity
SIN (Narrow)	Restricted Detection of valid Canadian social insurance numbers, tune in order to minimize false-positives. Requires additional evidences, such as SIN related terms (English or French) in proximity
SIN: with proximity	Detection of valid Canadian social insurance numbers, in proximity to social insurance related terms in English or French
Credit Cards: American Express	Detection of valid American Express credit card numbers employing various heuristics involving credit-card related terms and use of delimiters

Classifier	Description
Credit Cards: MasterCard	Detection of valid MasterCard credit card numbers employing various heuristics involving credit-card related terms and use of delimiters
Credit Cards: Visa	Detection of valid Visa credit card numbers employing various heuristics involving credit-card related terms and use of delimiters
Credit Cards: Visa with 13 digits	Detection of valid 13-digit Visa credit card numbers employing various heuristics involving credit-card related terms and use of delimiters
Credit Cards: Diners	Detection of valid Diners credit card numbers employing various heuristics involving credit-card related terms and use of delimiters
Credit Cards: Discover	Detection of valid Discover credit card numbers employing various heuristics involving credit-card related terms and use of delimiters
Credit Cards: Enroute	Detection of valid Enroute credit card numbers employing various heuristics involving credit-card related terms and use of delimiters
Credit Cards: JCB 1st	Detection of valid JCB credit card numbers employing various heuristics involving credit-card related terms and use of delimiters
Credit Cards: JCB 2nd	Detection of valid JCB credit card numbers employing various heuristics involving credit-card related terms and use of delimiters
Credit Cards: Bankcard	Detection of valid Bancard credit card numbers employing various heuristics involving credit-card related terms and use of delimiters
Credit Cards: Maestro, Switch or Solo	Detection of valid Maestro, Switch, or Solo credit card numbers employing various heuristics involving credit-card related terms in English and Russian, and use of delimiters
Brazilian Name	Detection of Brazilian full names
Brazil: CPF	Detection of CPF numbers, employing context-sensitive lexical analysis, statistical analysis of patterns, and custom dictionaries
Brazil: RG Numbers (Default)	Detection of RG (Registro Geral) numbers
Brazil: RG Numbers (Narrow)	Detection of RG (Registro Geral) numbers when appearing with support terms
Mexico RFC Number (Default)	Detection of Mexico RFC numbers, employing various heuristics involving RFC-related terms and homoclav
Mexico RFC Number (Wide)	Detection of of Mexico RFC numbers, without requiring homoclave or RFC term in proximity
IBAN General	Detection of general IBAN numbers

Classifier	Description
Credit Cards: Isracard	Detection of valid Isracard credit card numbers, when appearing together with an Isracard-related term in English or Hebrew. By default, only the last 4 digits are shown in the reports
ISIN: Default	Detection of valid International Securities Identification Numbers (ISINs)
ISIN: with country code validation	Detection of valid International Securities Identification Numbers (ISINs), validating country code
Australian TFN	Detection of an Australian Tax File (TFN) number, in proximity to TFN related terms
Singapore ID	Detection of Singapore NRIC, UIN and FIN identification numbers; does not require identification-related terms in proximity
Singapore ID with support	Detection of Singapore NRIC, UIN and FIN identification numbers, in proximity to identification-related terms
Japan Phone Numbers	Detection of least 10 Japanese telephone numbers, where at least one number is in proximity to phone number-related terms in English or Japanese
Japan Surnames	Detection of Japanese surnames
Driver License: Japan	Detection of Japanese Driver's License Number in proximity to driver license-related terms. The terms and digits are detected in both English and Japanese
Japan Pension	Detection of Japanese Pension Number in proximity to pension-related terms. The terms and digits are detected in both English and Japanese
Japan Ledger	Detection of Japanese Ledger Number in proximity to ledger-related terms. The terms and digits are detected in both English and Japanese
Japan Emails	Detection of at least 20 email addresses revealing personal information about the owner, such as their full name and place of employment
India: Form 16	Detection of India Form 16 that has been filled out, using identification of textual patterns common to such forms
South Korea ID	Detection of validated South Korea ID in a form like dddddd-ddddddd
South Korea ID - wide	Detection of validated South Korea ID, both delimited and non-delimited
Hong Kong: ID - non formal	Detection of Hong Kong ID of the form A1234567, without requiring ID terms
Hong Kong: ID - formal	Detection of Hong Kong ID of the form A123456(7)
Chinese Surnames	Detection of common Hong Kong surnames
Hong Kong: Address (Wide)	Detection of Hong Kong address, with possible false positives

Classifier	Description
Hong Kong: Address (Default)	Detection of Hong Kong address (default behavior)
Hong Kong: Address (Narrow)	Detection of Hong Kong address, tuned to minimize false positives (may cause false negatives)
Sweden ID - no support	Detection of validated Personal Identity Numbers; does not demand further evidence
New Zealand NHI - no support	Detection of validated NHI Numbers; does not demand further evidence
National Drug Code (Wide)	Detection of National Drug Code (NDC) numbers of prescription drugs in insulin products. All instances are returned and no further check is made; may cause false-positives
National Drug Code (Default)	Detection of National Drug Code (NDC) numbers of prescription drugs in insulin products. Undelimited numbers are subject to a statistical validation
National Drug Code (Narrow)	Detection of National Drug Code (NDC) numbers of prescription drugs in insulin products. At least 1 delimited number or 5 undelimited numbers, and both are subject to a statistical validation
US Address	Detection of US address
People’s Republic of China Identification Numbers	Detection of validated People's Republic of China Identification Numbers
Taiwan ID	Detection of validated Taiwan ID of the form A123456789
Taiwan ID with support	Detection of validated Taiwan ID of the form A123456789, providing that Taiwan ID terms in English or Chinese appears in proximity
Taiwan PII: Marital Status	Detection of Taiwan marital status
Taiwan PII: Birthday	Detection of Taiwan birthdays
Taiwan PII: Passport Numbers	Detection of passport numbers
Malaysia ID: with date validation	Detection of validated Malaysia ID in a form like YYMMDD-16-7356, where first six digits stand for a birthdate. Does not require support term in proximity
Malaysia ID: no date validation	Detection of validated Malaysia ID in a form like dddddd-16-7356. Does not require support term in proximity
Malaysia ID: with date validation and proximity	Detection of validated Malaysia ID in a form like YYMMDD-16-7356, where first six digits stand for a birthdate, providing that Malaysia ID terms such as MyKad, GMPC or ID appears in proximity
Malaysia ID: no date validation, with proximity	Detection of validated Malaysia ID in a form like dddddd-16-7356, providing that Malaysia ID terms such as MyKad, GMPC or ID appears in proximity
Malaysia ID: with date and BP validation	Detection of validated Malaysia ID in a form like YYMMDD-BP-7356, where first six digits stand for a birthdate. Does not require support term in proximity

Classifier	Description
Malaysia ID: with date and BP validation, and proximity	Detection of validated Malaysia ID in a form like dddddd-BP-7356, providing that Malaysia ID terms such as MyKad, GMPC or ID appears in proximity
US Age: smaller than	Detection of ages smaller than the age specified. Default age is 13.
US Age: greater than	Detection of ages greater than the age specified. Default age is 13.
US Phone Numbers	Detection of US phone numbers
Israeli Names	Detection of Israeli full names
Israel: General Medical Info	Detection of medical conditions in Hebrew or English.
Israel: Sensitive Medical Info	Detection of medical conditions of sensitive nature in Hebrew or English.
Israeli IBAN Wide	Detection of codes that belong to the ICD10 system. No additional information is required
ICD10 English Descriptions	Detection of English descriptions of medical conditions as appear in the ICD10 manual
ICD10 Norwegian Descriptions	Detection of Norwegian descriptions of medical conditions as appear in the ICD10 manual
Danish Account Numbers (Wide)	Detection of Danish bank account numbers
Danish Account Numbers (Default)	Detection of Danish bank account numbers, when found in proximity to bank account-related terms
Danish Account Numbers (Narrow)	Detection of strictly formatted Danish bank account numbers, when found in proximity to bank account-related terms
Denmark: CPR Number (Wide)	Detection of CPR numbers
Denmark: CPR Number (Default)	Detection of at least 5 CPR numbers, or at least 1 CPR + weak term ("CPR" for example)
Denmark: CPR Number (Narrow)	Detection of at least 1 Danish CC number with a term or at least 10 without
Thailand ID number (Wide)	Detection of at least 1 Thai ID number without support terms
Thailand ID number (Default)	Detection of at least 1 Thai ID number with support terms
Date Of Birth	Detection of dates of birth
Netherlands: Bank Account with proximity	Detection of Elfproef-validated Dutch bank account numbers, when found in proximity to bank account-related terms, such as "giropas"
Netherlands: Bank Account	Detection of Elfproef-validated Dutch bank account numbers.

Classifier	Description
Greece: AFM number (Default)	Detection of at least one Greek AFM number with a term in proximity, or several AFM numbers with statistical validation.
Greece: AFM number (Wide)	Detection of Greek AFM number with no term approvement or statistical validation.
Greece: Greek Name (Default)	Detection of Greek full name (default behavior).
Greece: Greek Name (Wide)	Detection of Greek full name (wide behavior).
Greece: Greek ID number	Detection of Greek ID number.
Finnish SSN (Default)	Detection of Finnish validated Social Security Numbers, when found in proximity to related terms.
Finnish SSN (Wide)	Detection of Finnish validated Social Security Numbers.
EIN (Default)	Detection of Employer ID Number (EIN).
Korea Phone Numbers (Wide)	Detection of Korea phone numbers.
Korea Phone Numbers (Narrow)	Detection of Korea phone numbers, employing statistical analysis.
Korea Phone Numbers (With Support)	Detection of Korea phone numbers, when found in proximity to related terms such as 'phone' in English or Korean.
NHS Numbers	Detection of validated NHS numbers.
CUSIP Numbers	Detection of validated CUSIP numbers.
Count Attachments (Stateful)	Detection of suspicious user behavior by aggregating the number of transactions of a specific file type sent by any single user.
Count CVs (Stateful)	Detection of suspicious user behavior by aggregating the number of transactions of curriculum vitae (CV) sent by any single user over a time. The number of transactions and the time period can be defined by the user.
Count Source Code Attachments (Stateful)	Detection of suspicious user behavior by aggregating the number of transactions of source code sent by any single user over a time. The number of transactions and the time period can be defined by the user.

Dictionaries

This section contains the full list of industry-related dictionaries provided by Websense.

Dictionary	Description
Non Acceptable Usage (Low)	Detection of low severity breaches of Acceptable Usage policy, with inappropriate language which is not explicit.
Non Acceptable Usage (Medium)	Detection of medium severity breach of Acceptable Usage policy, with mostly sexually oriented slang terms in multiple languages.
Non Acceptable Usage (High)	Detection of high severity breach of Acceptable Usage policy, with very explicit sexual terms or racial slurs.
Financial General: Unique	Detection of unique terms related to general financial data.
Financial General: Non-Unique	Detection of non-unique terms related to general financial data.
Financial General: Common	Detection of common terms related to general financial data.
Financial Investment: Unique	Detection of unique terms related to stocks, bonds, options, and other types of investment related financial data.
Financial Investment: Non-Unique	Detection of non-unique terms related to stocks, bonds, options, and other types of investment related financial data.
Financial Investment: Common	Detection of common terms related to stocks, bonds, options, and other types of investment related financial data.
Financial Personal: Unique	Detection of unique terms related to financial transactions, credit history, financial status, and other personal financial data.
Financial Personal: Non-Unique	Detection of non-unique terms related to financial transactions, credit history, financial status, and other personal financial data.
Financial Personal: Common	Detection of common terms related to financial transactions, credit history, financial status, and other personal financial data.
US Ethnicities	Detection of US name of a race or ethnicity.
Controlled Drugs	Detection of Controlled-drugs according to 21 CFR chapter III section 1308.
Strategic Documents: Unique	Detection of unique terms related to documents such as SWOT, business, or marketing plans.
Strategic Documents: Non-Unique	Detection of non-unique terms related to documents such as SWOT, business, or marketing plans.
Strategic Documents: Common	Detection of common terms related to documents such as SWOT, business, or marketing plans.
Strategic Documents: Attachments	Detection of MS Office attachments.

Dictionary	Description
Mergers and Acquisitions: Unique	Detection of unique Mergers and Acquisitions terms.
Mergers and Acquisitions: Common	Detection of common Mergers and Acquisitions terms.
Mergers and Acquisitions: Non-Unique	Detection of non-unique Mergers and Acquisitions terms.
Software Design: Non-Unique	Detection of non-unique terms related to design requirements, software architecture, user interface, and other software design related data.
Software Design: Common	Detection of common terms related to design requirements, software architecture, user interface, and other software design related data.
Software Design: Unique	Detection of unique terms related to design requirements, software architecture, user interface, and other software design related data.
Source Code: Verilog Phrases	Detection of terms and reserved words in Verilog.
Source Code: SPICE spectre	Detection of terms and reserved words in SPICE.
Pricing Terms	Detection of pricing-related terms.
	Detection of terms to support detection of pricing information.
Patents: Common	Detection of common patent terms.
Patents: Support	Detection of terms to support detection of patent applications.
Clinical Trials Confidential	Detection of terms that indicate confidential documents.
Clinical Trials	Detection of terms common in clinical trials information.
Itar: Encryption Terms	Detection of encryption related terms.
Itar: Military Terms	Detection of military related terms.
Itar: Nuclear Terms	Detection of nuclear related terms.
Itar: Space Terms	Detection of space related terms.
Ferc: Disclaimer	Detection of FERC do-not-release disclaimer.
Ferc: Pipeline Flow	Detection of terms related to FERC Natural gas pipeline flow diagrams and associated information.
Ferc: Pipeline support	Detection of terms related to FERC Natural gas pipeline flow diagrams and associated information.
Ferc: Form 567	Detection of terms related to FERC form 567 - Annual Report Of System Flow Diagrams and Capacity.
Ferc: Form 567 support	Detection of 'form 567' strings.
Ferc: Form 715	Detection of terms related to FERC form 715 - Annual Transmission Planning and Evaluation Report.

Dictionary	Description
Ferc: Form 715 support	Detection of 'form 715' strings.
SOX: Audit terms	Detection of SOX terms.
SOX: support	Detection of SOX terms.
ID support	Detection of ID number support terms.
Germany: Diseases	Detection of sensitive health condition in German or in English.
Germany: Ethnicities	Detection of name of a race or ethnicity, in German or English.
Germany: Crimes	Detection of name of a crime, in German or English.
Netherlands: Ethnicities	Detection of Dutch name of a race or ethnicity, in Dutch or English.
Netherlands: Crimes	Detection of name of a crime, in Dutch or English.
Netherlands: Diseases	Detection of sensitive health condition in Dutch or in English.
AHV support	Detection of AHV number support terms.
Norway: Diseases	Detection of sensitive health condition in Norwegian or in English.
Italy: Diseases	Detection of sensitive health condition in Italian or in English.
France: Diseases	Detection of sensitive health condition in French or in English.
Poland: PESEL support	Detection of Poland PESEL number support terms.
Poland: REGON support	Detection of Poland REGON number support terms.
Poland: IBAN support	Detection of Poland IBAN number support terms.
Driver License: Ireland support	Detection of Ireland DL number support terms.
Ireland: Passport support	Detection of Ireland passport number support terms.
US Sensitive Diseases	Detection of name of a disease, drug or a medical condition which is of a sensitive nature.
US Common Diseases	Detection of common diseases or health issues.
Greek Sensitive Diseases	Detection of Greek names of a diseases.
UK: Passport Number support	Detection of UK passport number support terms.
UK: Tax ID support	Detection of UK Tax ID number support terms.
Spain: Crimes	Detection of name of a crime, in Spanish or English.
Spain: Diseases	Detection of sensitive health condition in Spanish or in English.
Spain: Ethnicities	Detection of name of a race or ethnicity, in Spanish or English.

Dictionary	Description
California dictionary support	Detection of California dictionary support.
Colorado dictionary support	Detection of Colorado dictionary support.
Texas dictionary support	Detection of Texas dictionary support.
Washington dictionary support	Detection of Washington dictionary support.
US: Crimes	Detection of names of US crimes.
DNA support	Detection of DNA support terms.
Investment: Unique	Detection of unique terms related to stocks, bonds, options, and other types of investment financial data.
Investment: Common	Detection of common terms related to stocks, bonds, options, and other types of investment financial data.
Investment: Non-Unique	Detection of non-unique terms related to stocks, bonds, options, and other types of investment financial data.
Brazil: Diseases	Detection of Brazilian sensitive health condition in Portuguese or in English.
ISIN CAM support	Detection of 'CAM' strings.
ISIN support	Detection of ISIN related terms.
India PAN support	Detection of India PAN related terms.
Hong Kong: ID - support	Detection of Hong Kong ID related terms.
Macau ID - support	Detection of Macau ID related terms.
New Zealand: NHI support	Detection of NHI Numbers related terms.
Sweden ID support	Detection of Sweden ID related terms.
South Korea ID: support terms	Detection of South Korea ID number related terms.
Norway: First Names	Detection of Norwegian first names.
Norway: Last Names	Detection of Norwegian last names.
Denmark : CPR terms (wide)	Detection of Danish CPR wide terms.
Denmark : CPR terms (narrow)	Detection of Danish CPR narrow terms.
Energy: Prospecting Terms (High)	Detection of interesting prospecting terms (high severity).
Energy: Prospecting Terms (Medium)	Detection of interesting prospecting terms (medium severity).
Energy: Prospecting Terms (Low)	Detection of interesting prospecting terms (low severity).
Common passwords in English	Detection of common English passwords.
Filter - DOB	Filter for date of birth and age related terms.

Dictionary	Description
Filter - Passwords (dictionary)	Filter for passwords.
Patents Support Terms	Detection of patent related terms.
W-2 Form support terms 1	Detection of terms taken from the W-2 Form (Wage and Tax Statement).
IMEI - support terms	Detection of IMEI related terms.
Finnish SSN support terms	Detection of Finnish SSN support terms.
Denmark: First Name	Detection of Danish first names.
Denmark: Last Name	Detection of Danish last names.
Financial Terms	Detection of financial terms.
CV terms - Hebrew	Detection of CV terms in Hebrew.
UTM Terms	Detection of UTM (Universal Transverse Mercator) coordinate system terms.
EIN support terms	Detection of EIN related terms.
NHS numbers (support)	Detection of NHS related terms.
CUSIP Support terms	Detection of CUSIP related terms.
Physical Personal Terms	Detection of physical personal terms such as "Personal Data" and "Physical Characteristics".
Canadian Government ID Terms	Detection of Canadian Government ID terms such as "Canadian Government ID".
Canadian Permanent Resident Terms	Detection of Canadian Permanent Resident support terms such as "Permanent Card".
Canadian Indian Status Terms	Detection of Canadian Indian Status support terms such as "Indian Status".
Australian TFN Terms	Detection of Australian Tax File (TFN) related terms.
Japan Surnames ASCII	Detection of Japanese ASCII surnames.
Turkey TC Kimlik Terms	Detection of Turkey TC Kimlik terms.
Russian Passport Terms	Detection of Russian passport related terms.

PreciseID patterns

This section contains the full set of regular expression patterns provided by Websense.

Classifier	Description
Manuscript Terms 1	Detection of manuscript patterns.
Manuscript Terms 2	Detection of manuscript related terms.

Classifier	Description
Manuscript Terms 3	Detection of manuscript terms that support detection of manuscripts.
W-2 Form support terms 2	Detection of terms taken from the W-2 Form Header (like "FORM W 2" or "Form W-2").
CV support - period of years	Detection of a period denoted by starting year and ending year (e.g. 1999-2002).
Microsoft License Keys	Detection of Microsoft license keys.
Verilog Source Code - Entire Module Declaration	Detection of Verilog source code - looking for an entire Verilog module declaration.
Verilog Source Code - Module Header Declaration	Detection of Verilog source code - looking for Verilog module declaration (header only).
VHDL Source Code - Declaration Footer	Detection of VHDL source code - looking for a terminating declaration of Architecture, Component, Process or Entity.
VHDL Source Code - Use Statement	Detection of VHDL source code - looking for a use statement declaration.
SPICE Source Code - Constant Declaration	Detection of constants declaration in the SPICE programming language.
SPICE Source Code - Sub-Circuit Declaration	Detection of a Sub-Circuit declaration in the SPICE programming language.
SPICE Source Code - Various Key Words 1	Detection of various keywords in the SPICE programming language.
SPICE Source Code - Various Key Words 2	Detection of various keywords in the SPICE programming language.
SPICE Source Code - Various Key Words 3	Detection of various keywords in the SPICE programming language.
SPICE Source Code - Simulator Langugae Declaration	Detection of a SPICE simulator language declaration.
US Price	Detection of a price in dollars.
Clinical Trial Numbers	Detection of numbers likely to appear in 'Clinical Trial' documents.
Confidential Header/Footer	Detection of documents with terms indicating confidentiality in the header or footer.
Energy Logs and Survey Reports	Detection of terms related to Prospecting Logs and Survey Reports.
Network Terms and IP Addresses	Detection of network related terms and IP addresses.
Network Terms	Detection of network related terms.
IP Address - Wide	Detection of all possible forms of IP addresses.
IP Address - Narrow	Detection of an IP address, when found in proximity to IP related term such as 'IP' or 'subnet'.
IP Address	Detection of an IP Address.

Classifier	Description
Russian Passport - significant	Detection of a Russian passport with a passport term in proximity
account 5 to 8 digits	Detection of 5-8 digit account numbers.
Swiss AHV Number (New Format)	Detection of a Swiss AHV (Swiss Social Security) number in its new format (introduced at July 1st, 2008).
Swiss AHV Number (Old Format)	Detection of a Swiss AHV (Swiss Social Security) number in its old format.
Polish Name	Detection of a Polish name.
Polish NIP support terms	Detection of terms related to Polish NIP number (a number used for tax identification).
Polish ID support terms	Detection of terms related to Polish ID number.
Irish Drivers License	Detection of Irish driver's license.
Irish PPS Terms	Detection of terms related to Irish PPS (Personal Public Service) number.
UK National Insurance Number	Detection of a UK national insurance number (NINO).
UK National Insurance Number - no proximity	Detection of a UK national insurance number (NINO) without terms in proximity.
EU National Insurance Number	Detection of various European national insurance number formats (UK NINO, French INSEE, Spanish DNI, Italian Codice Fiscale).
5-9 Digit Account Number	Detection of any 5-9 digit account numbers.
5-8 Digit Account Number with support	Detection of any 5-8 digit number in proximity to an account number support term (can be used for various account types as long as they are 5-8 digits).
9 Digit Account Number with support	Detection of any 9 digit number in proximity to an account number support term (can be used for various account types as long as they are 9 digits).
10 Digit Account Number with support	Detection of any 10 digit number in proximity to an account number support term (can be used for various account types as long as they are 10 digits).
UK Passport number	Detection of a UK passport number.
UK Tax ID	Detection of a UK tax ID number.
IL Insurance: Claim support	Detection of terms to support identification of an Israeli Insurance Claim Number.
Account and Password	Detection of a 5-10 digit account number, in proximity to a password with a password related term next to it.
IL Insurance Policy: 8 digits	Detection of 8 digit policy numbers.
IL Insurance Policy: 10 digits	Detection of 10 digit policy numbers.
IL Life Insurance support	Detection of insurance terms in Hebrew.

Classifier	Description
IL Insurance: Generic with proximity	Detection of a generic Israeli Insurance Number with terms in proximity.
IL Insurance Policy: 10 digits - support	Detection of 10 digits Israeli Insurance Number with terms in proximity.
Account Number 6-13 digits	Detection of 6-13 digit account numbers.
Account Number Terms Hebrew and English Support	Detection of account terms in English or Hebrew.
Account Number 5-9 digits, with Hebrew or English Support	Detection of any 5-9 digit account numbers, when found in proximity to account related terms in English or Hebrew.
IL buy or sell instructions	Detection of buy and sell instructions in Hebrew.
IL buy or sell instructions support	Detection of buy and sell support instructions in Hebrew.
Australia: Medicare	Detection of Australian Medicare numbers, each in proximity to Medicare related terms.
Driver License: Australia	Detection of Australian driver license.
Driver License Support	Detection of driver license support terms.
Driver License: Arkansas	Detection of Arkansas driver license.
Driver License: Arizona	Detection of Arizona driver license.
Driver License: California	Detection of California driver license.
Driver License: Colorado	Detection of Colorado driver license.
Driver License: Connecticut	Detection of Connecticut driver license.
Driver License: Florida	Detection of Florida driver license.
Driver License: Georgia	Detection of Georgia driver license.
Driver License: Illinois	Detection of Illinois driver license.
Driver License: Minnesota	Detection of Minnesota driver license.
Driver License: New Jersey	Detection of New Jersey driver license.
Driver License: New York	Detection of New York driver license.
Driver License: North Carolina	Detection of North Carolina driver license.
Driver License: Ohio	Detection of Ohio driver license.
Driver License: Pennsylvania	Detection of Pennsylvania driver license.
Driver License: Texas	Detection of Texas driver license.
Driver License: Washington	Detection of Washington driver license.
Driver License: Wisconsin	Detection of Wisconsin driver license.
Driver License: Michigan	Detection of Michigan driver license.

Classifier	Description
Driver License: US all patterns	Detection of various US driver license formats.
Arizona dictionary support	Detection of Arizona support terms.
Illinois: State ID	Detection of Illinois state ID.
Minnesota dictionary support	Detection of Minnesota support terms.
New York dictionary support	Detection of New York support terms.
DNA pattern	Detection of DNA patterns.
US Grades	Detection of grades in proximity to an academic subject.
Zip Plus 4	Detection of Zip codes.
US ITIN	Detection of Individual Taxpayer Identification Number (ITIN).
Credit Cards: Isracard support	Detection of Isracard Credit Card support terms (Hebrew and English).
Japan: Account 1st Format	Detection of a Japanese account number.
Japan: Account	Detection of a Japanese account number.
India: PAN	Detection of Indian PAN number.
Macau ID - formal	Detection of Macau ID number (formal form).
Macau ID - non formal	Detection of Macau ID number (non formal form).
Password Terms	Detection of password related terms.
Explicit Password	Detection of explicit password information (e.g. "password is xxxx").
General Password	Detection of passwords comprised of at least 5 characters (must include both letters and digits).
Password as URL parameter	Detection of password as URL parameter.
Energy File Extensions	Detection of files containing petrophysical data.
Source Code Extensions	Detection of C and Java files according to their extension.
UTM distances	Detection of numbers representing distance in meters as used in the UTM coordinate system.
EIN pattern	Detection of Employer ID Numbers (EIN).
Netherlands: Bank Account Terms	Detection of Dutch Bank Account related terms.
Physical Information - Blood Type	Detection of Private Physical Information - Blood Type.
Physical Information - Eye Color	Detection of Private Physical Information - Eye Color.
Physical Information - Hair Color	Detection of Private Physical Information - Hair Color.

Classifier	Description
Physical Information - Sex	Detection of Private Physical Information - Sex.
Physical Information - Build	Detection of Private Physical Information - Build.
Physical Information - Complexion	Detection of Private Physical Information - Complexion.
Physical Information - Height	Detection of Private Physical Information - Height.
Physical Information - Weight	Detection of Private Physical Information - Weight.
Canadian Government ID	Detection of Canadian Government IDs.
Canadian Permanent Resident	Detection of Canadian Permanent Resident Numbers.
Canadian Indian Status	Detection of Canadian Indian Status Numbers.
Brazil: RG Numbers Terms	Detection of RG (Registro Geral) related terms.
Singapore ID Terms	Detection of Singapore NRIC related terms.
India: Form 16 Headings	Detection of India Form 16 headings.
Iceland SSN Terms	Detection of Iceland identification numbers (kennitala) related terms.
CV in Russian or Ukraine support terms	Detection of curriculum vitae in Russian or Ukrainian with support terms.
Japan Surnames Unicode	Detection of Japanese Unicode .

C Supported File Formats

This appendix provides a list of all the file formats that Websense Data Security supports for defining file type policies.

The file formats supported are constantly being updated and added to.

For further information, see *Adding a file-type classifier*, page 80.

File Type	Description
Ability Comm	Communication Ability
Ability DB	Database Ability
Ability Image	Raster Image Ability
Ability SS	Spreadsheet Ability
Ability WP	Word Processor Ability
ASF	Advanced Systems Format
ACT	ACT
AES Multiplus Comm	Multiplus (AES)
AIFF	Audio Interchange File Format (AIFF)
ALIS	ALIS
Amiga IFF 8SVX	Amiga IFF (8SVX) Sound
Amiga MOD	Amiga MOD
Apple Double	Apple Double
Apple Single	Apple Single
Applix Alsterix	Applix Alsterix
Applix Graphics	Applix Graphics
Applix Spreadsheets	Applix Spreadsheets
Applix Words	Applix Words
ARC PAK Archive	PAK/ARC Archive
ASCII Text	Text
AU Audio	NeXT/Sun Audio Data

File Type	Description
AutoCAD DXF Binary	AutoCAD DXF
AutoCAD DXF Text	AutoCAD DXF
AutoDesk Animator FLI	AutoDesk Animator FLIC
AutoDesk AnimatorPro FLC	AutoDesk Animator Pro FLIC
AutoDesk DWG	AutoDesk Drawing (DWG)
AutoDesk WHIP	AutoDesk WHIP
AutoShade Rendering	AutoShade Rendering
BinHex	BinHex
BMP	Windows Bitmap
CAB	Microsoft cabinet (CAB) files
CADAMCAB	CADAM Drawing
CADAM	CADAM Drawing Overlay
CDA DDIF	CDA / DDIF
CEOwrite	CEOwrite
CGM Binary	Computer Graphics Metafile (CGM)
CGM Character	Computer Graphics Metafile (CGM)
CGM ClearText	Computer Graphics Metafile (CGM)
COMET TOP Word	COMET TOP
Compactor Archive	Compactor / Compact Pro
Compress	Unix Compress
Corel Draw	Corel Draw
Corel Draw CMX	Corel CMX
Corel Presentations	Corel Presentations
CPT Comm	CPT
Creative Voice Audio	Creative Voice (VOC)
CSV	CSV (Comma Separated Values)
CT DEF	Convergent Technologies DEF Comm. Format
Curses Screen	Curses Screen Image
Data Point VistaWord	Vistaword
dBase Database	dBase Database
DCA RFT	DCA-RFT (IBM Revisable Form)
DCS	DCS
DCX FAX format	DCX FAX Format(PCX images)
DECdx	DECdx

File Type	Description
DeVice Independent	DeVice Independent file (DVI)
DG CDS	DG Common Data Stream (CDS)
Dicom	digital imaging and communications in medicine, “.dcm”. Rasterimage.
DIF SpreadSheet	Data Interchange Format (DIF)
Disk Doubler	Disk Doubler
DSA101	DSA101 (Honeywell Bull)
EBCDIC	EBCDIC Text
ELF Dynamic Lib	ELF Dynamic Library
ELF Executable	ELF Executable
ELF Relocatable	ELF Relocatable
Enable Spreadsheet	Enable Spreadsheet
Enable WP	Enable Word Processing
EnCase	Expert witness compression format, “.e01”, “.l01”, etc. Encapsulation file.
Enhanced Metafile	Enhanced Metafile
Envoy	Envoy
Encapsulated PostScript	Encapsulated PostScript (raster)
FileMaker Mac	Filemaker MAC
Folio Flat	Folio Flat File
FPX	FPX Format
FrameMaker	FrameMaker
FrameMaker Book	FrameMaker
Framework	Framework
Framework II	Framework II
Freehand	Freehand MAC
Freelance 96	Lotus Freelance 96
Freelance 97	Lotus Freelance 97
Freelance DOS	Lotus Freelance for DOS
Freelance OS2	Lotus Freelance for OS/2
Freelance Win	Lotus Freelance for Windows
FTP Software Session	FTP Session Data
G31D	CCITT G3 1D
GEM Image	GEM Bit Image
GEM VDI	GEM VDI

File Type	Description
GIF 87a	Graphics Interchange Format (GIF87a)
GIF 89a	Graphics Interchange Format (GIF89a)
GZ Compress	GZ Compress
Harvard Graphics	Harvard Graphics
Harvard Graphics Cfg	Harvard Graphics Configuration File
Harvard Graphics Chart	Harvard Graphics Chart
Harvard Graphics Palette	Harvard Graphics Palette
Harvard Graphics Symbol	Harvard Graphics Symbol File
Hl7	Health level 7 message
HP GL	HP Graphics Language
HP Graphics Language	HP Graphics Language (Plotter)
HP PCL	HP Printer Control Language
HP Word PC	HP Word PC
HTML	HTML
HWP	HWP(Arae-Ah Hangul)
IBM 1403 LinePrinter	IBM 1403 Line Printer
IBM DCA FFT	DCA-FFT (IBM Final Form)
IBM DCF Script	DCF Script
IBM Display Write	Display Write
IBM Writing Assistant	IBM Writing Assistant
ICHITARO	ICHITARO V4-10
IFilter	Ifilter wordprocessing file
Intergraph V7 DGN	Intergraph Standard File Format (ISFF) V7 DGN (non-OLE)
Interleaf	Interleaf
IS XML	Verity XML
JPEG File Interchange	JPEG Interchange Format
Lasergraphics Language	Lasergraphics Language
LHA	LHA Archive
Lotus 123 97	Lotus 1-2-3 97
Lotus 123 Format	Lotus 1-2-3 Formatting
Lotus 123 R9	Lotus 1-2-3 Release 9
Lotus 123 Worksheet	Lotus 123 Worksheet
Lotus Ami Pro	Lotus Ami Pro
Lotus Ami Pro Draw	Lotus Ami Pro Draw

File Type	Description
Lotus Ami Pro StyleSheet	Lotus Ami Pro Style Sheet
Lotus Notes BitMap	Lotus Notes Bitmap
Lotus Notes CDF	Lotus Notes CDF
Lotus Notes NSF	IBM Lotus Notes Database NSF/NTF
Lotus PIC	Lotus PIC
Lotus ScreenCam	Lotus ScreenCam
Lotus Word Pro 96	Lotus Word Pro 96
Lotus Word Pro 97	Lotus Word Pro 97
Lyrix	Lyrix Word Processing
Mac PICT	QuickDraw Picture
MacBinary	MacBinary
MacPaint	MacPaint
Macromedia Director	Macromedia Director
Macromedia Flash	SWF
MacWrite	MacWrite
MacWrite II	MacWrite II
Maker Interchange	Maker Interchange Format (MIF)
Maker Markup Language	Maker Markup Language
MASS 11	MASS-11
Micrografx Designer	Micrografx Designer
Micrografx Draw	Windows Draw (Micrografx)
MicroStation V8 DGN	MicroStation V8 DGN (OLE)
MIDI Audio	MIDI
MIME HTML	MIME HTML
MORE	MORE Database MAC
MPEG-1 Video	MPEG Video
MPEG Audio	MPEG Audio
MS Access	Microsoft Access
MS Access 2000	Microsoft Access 2000
MS Access 95	Microsoft Access 95
MS Access 97	Microsoft Access 97
MS ASF	Microsoft ASF file
MS COM Executable	PC (.COM)
MS DIB	MS Windows Device Independent Bitmap
MS Excel 2007	Microsoft Excel 2007 XML

File Type	Description
MS Excel XML	Microsoft Excel XML
MS Excel	Microsoft Excel
MS Excel 2000	Microsoft Excel 2000
MS Excel 95	Microsoft Excel 95
MS Excel 97	Microsoft Excel 97
MS Excel Chart	Microsoft Excel
MS Excel Encrypted	Encrypted Excel
MS Excel Macro	Microsoft Excel
MS Executable	MSDOS/Windows Program
MS Help File	Microsoft Help File
MS Office Drawing	Microsoft Office Drawing
MS Outlook	Microsoft Outlook
MS OutlookPST	Microsoft Outlook PST
MS Pocket Word	Microsoft Pocket Word
MS PPT 2007	Microsoft PPT 2007 XML
MS Project 2000	Microsoft Project 2000
MS Project 4	Microsoft Project 4
MS Project 41	Microsoft Project 4.1
MS Project 98	Microsoft Project 98
MS Project 2007	Microsoft Project 2007
MS Project Activity	Microsoft Project
MS Project Calc	Microsoft Project
MS Project Resource	Microsoft Project
MS Publisher 98	Microsoft Publisher 98
MS RTF	Rich Text Format (RTF)
MS TNEF	MS TNEF
MS Video	Video for Windows (AVI)
MS Visio	Microsoft Visio
MS Visio XML	Microsoft Visio XML
MS WAVE Audio	Microsoft Wave
MS Windows Write	Windows Write
MS Word 2000	Microsoft Word 2000
MS Word 2007	Microsoft Word 2007 XML
MS Word 95	Microsoft Word 95
MS Word 97	Microsoft Word 97

File Type	Description
MS Word Mac	Microsoft Word for Macintosh
MS Word PC	Microsoft Word for PC
MS Word PC Driver	Microsoft Word for PC Driver
MS Word PC Glossary	Microsoft Word for PC Glossary
MS Word PC Misc	Microsoft Word for PC Miscellaneous File
MS Word PC StyleSheet	Microsoft Word for PC Style Sheet
MS Word UNIX	Microsoft Word UNIX
MS Word Win	Microsoft Word for Windows
MS Word XML	Microsoft Word XML
MS Works DOS DB	Microsoft Works for DOS
MS Works DOS SS	Microsoft Works for Windows
MS Works DOS WP	Microsoft Works for DOS
MS Works Mac Comm	Microsoft Works for MAC
MS Works Mac DB	Microsoft Works for MAC
MS Works Mac SS	Microsoft Works for MAC
MS Works Mac WP	Microsoft Works for MAC
MS Works Win DB	Microsoft Works for Windows
MS Works Win SS	Microsoft Works for Windows
MS Works Win WP	Microsoft Works for Windows
MS-DOS Batch File	MS-DOS Batch File
MS-DOS Device Driver	MS-DOS Device Driver
Multimate	MultiMate
Multimate Adv	MultiMate Advantage
Multimate Adv Fnote	MultiMate Advantage Footnote File
Multimate Adv II	MultiMate Advantage II
Multimate Adv II Fnote	MultiMate Advantage II Footnote File
Multimate Fnote	MultiMate Footnote File
Multiplan Mac	Multiplan (Mac)
Multiplan PC	Multiplan (PC)
Navy DIF	Navy DIF
NBI Async Archive	NBI Async Archive Format
NBI Net Archive	NBI Net Archive Format
Netscape Bookmark File	Netscape Bookmark File
NeWS Font	NeWS bitmap font
NIOS TOP	NIOS TOP

File Type	Description
NURSTOR Drawing	NURSTOR Drawing
Oasis	Oasys format
ODA Q1 11	ODA / ODIF
ODA Q1 12	ODA / ODIF
ODIF FOD26	ODA / ODIF
ODIF FOD36	ODA / ODIF
Office Writer	Office Writer
OLE	OLE Compound Document
OLE DIB	OLE DIB object
OLIDIF	OLIDIF (Olivetti)
OneNote	Word processing note format ".one" from OneNote
OpenPGP	OpenPGP Message Format
OS/2 PM Metafile	OS/2 PM Metafile
PageMaker Mac	PageMaker for Macintosh
PageMaker Win	PageMaker for Windows
Paradox	Paradox Database
PBM ASC	Portable Bitmap Utilities ASCII Format
PBM BIN	Portable Bitmap Utilities Binary Format
PC Library	DOS/Windows Object Library
PC Obj	DOS/Windows Object Module
PC Paintbrush	PC Paintbrush Graphics (PCX)
PCD	PCD Format
PDF	Portable Document Format
PDF Encrypted	Encrypted PDF Document
PeachCalc	PeachCalc
Persuasion	Persuasion
PEX Binary Archive	SUN PEX Binary Archive
PGM ASC	Portable Greymap Utilities ASCII Format
PGM BIN	Portable Greymap Utilities Binary Format
PGP ASCII Encoded	ASCII-armored PGP encoded
PGP ASCII Public Keyring	ASCII-armored PGP Public Keyring
PGP ASCII Signed	ASCII-armored PGP encoded
PGP Compressed Data	PGP Compressed Data
PGP Encrypted Data	PGP Encrypted Data

File Type	Description
PGP Public Keyring	PGP Public Keyring
PGP Secret Keyring	PGP Secret Keyring
PGP Sign Certificate	PGP Signature Certificate
PGP Signed Data	PGP Signed Data
PGP SignedEncrypted Data	PGP Signed and Encrypted Data
Philips Script Word	Philips Script
PKZIP	ZIP Archive
PlanPerfect	PlanPerfect
PNG	Portable Network Graphics (PNG)
PostScript	PostScript
PowerPoint 2000	Microsoft PowerPoint 2000
PowerPoint 95	Microsoft PowerPoint 95
PowerPoint 97	Microsoft PowerPoint 97
PowerPoint Mac	Microsoft PowerPoint for Macintosh
PowerPoint Win	Microsoft PowerPoint for Windows
PPM ASC	Portable Pixmap Utilities ASCII Format
PPM BIN	Portable Pixmap Utilities Binary Format
Preview EPSF	Encapsulated PostScript
PRIMEWORD	PRIMEWORD
Q & A for DOS	Q & A for DOS
Q & A for Windows	Q & A for Windows
Quadratron Q One v1	Q-One V1.93J
Quadratron Q One v2	Q-One V2.0
Quark Xpress	Quark Xpress MAC
Quattro Pro DOS	Quattro Pro for DOS
Quattro Pro Win	Quattro Pro for Windows
QuickDraw 3D Metafile	QuickDraw 3D Metafile
QuickTime	QuickTime Movie
RAR	RAR
Real Audio	Real Audio
Reflex	Reflex
RIFF DIB	RIFF Device Independent Bitmap
RIFF MIDI	RIFF MIDI
RIFF Multimedia Movie	RIFF Multimedia Movie

File Type	Description
SAMNA Word IV	SAMNA Word
Scrap	Shell scrap object file, “.shs”. Encapsulation file.
Skype	Skype log file.
SFX	FMT Self Extracting Archive
SGI Image	SGI Image
SGML	SGML
SmartWare II Comm	SmartWare II
SmartWare II DB	SmartWare II
SmartWare II SS	SmartWare II
SmartWare II WP	SmartWare II
SMTP	SMTP
SO Presentation XML	StarOffice Presentation XML
SO Spreadsheet XML	StarOffice Spreadsheet XML
SO Text XML	StarOffice Text XML
SOF Encapsulation	Serialized Object Format (SOF)
StuffIt	StuffIt (MAC)
Sun Raster	Sun Raster
Sun vfont	SUN vfont Definition
SuperCalc	Supercalc
SVF	Simple Vector Format (SVF)
SYLK Spreadsheet	SYLK
Symphony	Symphony
TAR	TAR
Targa	Targa
Targon Word	Targon Word
TIFF	TIFF
TrueType Font	TrueType Font
UltraCalc	UltraCalc
Unicode	Unicode
Uniplex Ucalc	Uniplex Ucalc
Uniplex WP	Uniplex
UNIX Exe 3B20	Unix Executable (3B20)
UNIX Exe Basic 16	Unix Executable (Basic-16)
UNIX Exe Bell 5	Unix Executable (Bell 5.0)
UNIX Exe iAPX 286	Unix Executable (iAPX 286)

File Type	Description
UNIX Exe MC68k	Unix Executable (MC680x0)
UNIX Exe PreSysV VAX	Unix Executable (PDP-11/pre-System V VAX)
UNIX Exe VAX	Unix Executable (VAX)
UNIX Exe WE32000	Unix Executable (WE32000)
UNIX Exe x86	Unix Executable (x86)
UNIX Obj MS8086	Unix Object Module (old MS 8086)
UNIX Obj VAX Demand	Unix Object Module (VAX Demand)
UNIX Obj Z8000	Unix Object Module (Z8000)
UNIX SHAR	SHAR
Unknown	Unknown File Format
USENET	USENET
UUEncoded	UU encoded
Volkswriter	Volkswriter
VRML	VRML
Wang GDL	WANG Office GDL Header
WANG PC	WANG PC
WANG WITA	WANG WITA
WANG WPS Comm	WANG WPS
Windows Animated Cursor	Windows Animated Cursor
Windows CPP Obj Storage	Windows C++ Object Storage
Windows Cursor	Windows Cursor
Windows Group	Windows Group
Windows Help	Windows Help File
Windows Icon	Windows Icon Format
Windows Metafile	Windows Metafile
Windows Metafile NoHdr	Windows Metafile (no header)
Windows Palette	Windows Palette
Windows PIF	Program Information File (PIF)
WMA	Windows Media Audio Format
WMV	Windows Media Video Format
Word Connection	Word Connection
Word Encrypted	Encrypted MS Word
WordERA	WordERA
WordMARC	WordMARC

File Type	Description
WordPerfect	WordPerfect
WordPerfect Auxiliary	WordPerfect auxiliary file
WordPerfect Cfg	WordPerfect Configuration File
WordPerfect Dictionary	WordPerfect Spelling Dictionary
WordPerfect Driver	WordPerfect Driver
WordPerfect Graphics	WordPerfect Graphics
WordPerfect Hyphenation	WordPerfect Hyphenation Dictionary
WordPerfect Mac	WordPerfect MAC
WordPerfect Macro	WordPerfect Macro
WordPerfect Misc	WordPerfect Miscellaneous File
WordPerfect Resource	WordPerfect Resource File
WordPerfect Thesaurus	WordPerfect Thesaurus
WordPerfect VAX	WordPerfect VAX
WordStar	WordStar
WordStar 2000	WordStar 2000
WPS PLUS	WPS-PLUS
WriteNow	WriteNow MAC
XBM	X Bitmap Format
Xerox 860 Comm	Xerox 860
Xerox Writer	Xerox Writer
XHTML	XHTML
XML	XML
XPM	X Pixmap Format
XyWrite	XYWrite / Nota Bene
ZIP Encrypted	Encrypted Zip archive

D Endpoint Applications

You can monitor any number of applications on the endpoint. Websense has analyzed the metadata for dozens of applications and can monitor these with great accuracy. (They are listed below.) You can add other applications to the list. If you want to analyze the applications based on their metadata, you can use utility that Websense provides.

Built-in support

Following are the applications that you can choose to monitor on the endpoint when you set up your endpoint policy. This includes software applications, Web applications, and SaaS (software as a service) applications.

- 7-Zip File Manager - 7-Zip
- Acoustica MP3 CD Burner - Acoustica MP3 CD Burner
- Adobe Reader 8.1 - Adobe Reader
- Alcohol 120% - Alcohol 120%
- Alcohol Launcher - Alcohol Soft Development Team
- Ares p2p for windows - Ares p2p for windows
- AX-Crypt Encryption Software - AX-Crypt
- Azureus - Azureus
- BearShare - BearShare
- BitComet - a BitTorrent Client - BitComet
- BitLord - BitLord
- Bittorrent
- Bluetooth Stack COM Server - BTStackServer
- btdownloadgui
- CD Mate - CD Mate
- Core FTP App - Core FTP
- CuteFTP File Transfer Application - CuteFTP Home
- DK2 Network Server Remote Monito - DK2 DESkey
- eMule - eMule

- EUDORA - Eudora
- EUDORA - Eudora Light
- EUDORA - Eudora Pro
- File Encryption XP - File Encryption XP
- File encryption/decryption/wipin - File Waster
- FileZilla FTP Client - filezilla
- FineCrypt Control Center - FineCrypt (R)
- Firefox - Firefox
- FlashFXP - FlashFXP
- FrostWire - FrostWire
- Fsquirt - Fsquirt
- FTP Voyager®, an FTP Client for - FTP Voyager®
- Google Talk - Google Talk
- ICQ Library - ICQ
- ICQLite - ICQLite
- Internet Explorer - Microsoft(R) Windows (R) 2000 Operating System
- Internet Explorer - Microsoft® Windows® Operating System
- Internet Explorer - Windows® Internet Explorer
- Kazaa download/database viewer a - K-Dat
- Kazaa QuickLinks Handler/Generat - K-Sig
- klrun: protocol - KL Extensions
- LeechFTP - LeechFTP
- LimeWire - LimeWire
- Lotus Notes
- Messenger - Messenger
- Microsoft Office 2007:
  - Access
  - Communicator
  - Excel
  - InfoPath
  - OneNote
  - Outlook
  - Outlook Mobile Manager
  - PowerPoint
  - Project
  - Publisher
  - Visio
  - Word

    - Outlook Mobile Manager
- Microsoft Office 2003:
    - Access
    - Excel
    - OneNote
    - Outlook
    - Outlook Mobile Manager
    - Powerpoint
    - Project
    - Publisher
    - Visio
    - Word
- Mozilla Thunderbird - Thunderbird
- MXit PC v1.2 - MXit PC
- Nero Burning ROM - Nero Burning ROM
- Notepad - MS Windows Operating System
- Office Communicator 2005 - Microsoft Office Communicator 2005
- OpenOffice.org Suite
- Opera Internet Browser - Opera Internet Browser
- Outlook Express - Microsoft(R) Windows (R) 2000 Op
- Outlook Express - Microsoft(R) Windows NT(R) Opera
- Outlook Express - Microsoft® Windows® Operating Sy
- pando - pando
- Pegasus Mail for Windows
- Pegasus Mail WSENDTO Utility
- psi
- QQ - QQ
- Roxio Creator Classic - Creator Classic
- Safari Web Browser - Safari
- Serv-U File Server EXE - Serv-U File Server
- Serv-U File Server Tray Applicat - Serv-U File Server
- Serv-U FTP Server Setup Utility - Serv-U File Server
- Skype - Skype
- SmartFTP Client - SmartFTP Client
- Steganos LockNote - Steganos LockNote
- uTorrent
- Windows Live Messenger - Messenger
- Windows Mail

- Windows Messenger - Messenger
- Windows Privacy Tray (WinPT) - Windows Privacy Tray
- WinRAR archiver
- WinZip - WinZip
- Wireless Link File Transfer App - Irftp
- WordPad MFC Application - MS Windows Operating System
- WS_FTP Pro Application - WS_FTP Professional
- Yahoo! Messenger - Yahoo! Messenger
- YServer Module - Yahoo! Messenger

Importing other applications

There are 2 ways to import applications onto the Data Security server if you want to monitor an endpoint application other than the ones supplied by Websense:

1. Selecting **Main** > **Resources** > **Applications** > **New Application/ Online Application**. See *Endpoint Applications*, page 109.

   When you add applications using this screen, they are identified by their executable name. Occasionally, users try to get around being monitored by changing the executable name. For example, if you're monitoring "winword.exe" on users' endpoint devices, they may change the executable name to "win-word.exe" to avoid being monitored.

2. Using an external utility program, **DSSRegApps.exe**. This method records the application's metadata, so that Websense Data Security can analyze the metadata.

In other words, if the name of the application is modified by an end users, Websense Data Endpoint can still identify the application and apply policies.

> ✓ **Note**
>
> This tool can be copied to any other machine and be executed on it as long as it has connectivity to the Data Security Management Server.

To use the external tool to import applications in the Data Security server:

1. Go to [%DSS_Home%] directory (Default: C:\Program Files\Websense\Data Security Suite) and double-click **DSSRegApps.exe**. The Get File Properties screen is displayed.

2. Complete the following fields:

Field	Description
IP Address/ Hostname	Insert the IP Address or Hostname of the Data Security Server.
User Name	Provide the user name used to access the Data Security Server. This is the user name assigned to administrators that have relevant permissions.
Password	Enter the Password used to access the Data Security Server. This is the password assigned to administrators with relevant permissions
File Name	Insert the File Name of the application, e.g. Excel.exe OR click the Browse… button and in the Open dialog box, navigate to the File Name of the application and double-click it.
Display Name	Enter the name of the application as you want it displayed in the Data Security Management Server.

3. Click **OK**.

A message will appear indicating that the application was successfully registered with the Data Security Server. The Get File Properties screen will be re-displayed with the Data Security Server fields completed, but the File Name and Display Name empty. This allows you to select additional applications to register with the Data Security Server. Continue this process until all applications are registered. When you are finished adding applications, click the Cancel button in the Get File Properties screen.

E

File Size Limits

This appendix lists the file size limitations for network, endpoint, and data discovery functions in Websense Data Security. See the key after the table for a description of each column.

Channel	Analysis Timeout (sec)	Max Intercepted Size (MB)	Max Extracted Sub-Files (total in MB)	Max Extracted Sub-Files (count)	Extracted Text Size Per File (MB)	Max Forensics (MB)
Network						
SMTP inline (pama, SMTP, Exchange)	35	100	100	100	1	Unlimited
SMTP monitoring (pama, SMTP, Exchange)	300	100	100	100	1	Unlimited
HTTP (inline, ICAP, ISA, WCG)	10	12	100	100	1	12
HTTP (Monitoring)	300	100	100	100	1	12
IM	300	100	100	100	1	12
FTP	300	100	100	100	1	Unlimited
FTP “inline” (through ICAP and WCG)	10	12	100	100	1	12
Print (blocking)	10	12	N/A	N/A	1	12
Print (monitoring)	300	12	N/A	N/A	1	12
Endpoint						

Channel	Analysis Timeout (sec)	Max Intercepted Size (MB)	Max Extracted Sub-Files (total in MB)	Max Extracted Sub-Files (count)	Extracted Text Size Per File (MB)	Max Forensics (MB)
Copy to Removable Media	25	Unlimited*	100	100	1	12
Copy over LAN	25	Unlimited*	100	100	1	12
File Access	25	Unlimited*	100	100	1	12
Copy-Cut	5	Unlimited*	N/A	N/A	1	12
Paste	5	Unlimited*	N/A	N/A	1	12
Screen Capture	N/A	N/A	N/A	N/A	N/A	12
Print	25	300*	N/A	N/A	1	12
HTTP	10	Unlimited*	100	100	1	12
Web Download	25	Unlimited*	100	100	1	12
Discovery						
Network Discovery	Unlimited *	Unlimited*	50	100	1	N/A
Endpoint Discovery	Unlimited *	Unlimited*	50	100	1	N/A

*Unlimited - Files beyond 100 MB are searched only for file name, file size, and binary fingerprint. The binary fingerprinting is based on 10 MB from the file.

Key

- **Analysis Timeout (sec):** Maximum analysis timeout (seconds). When the different agents submit a transaction to be analyzed by the policy engine, they specify how much time the policy engine has to analyze. At the end of this time, the policy engine returns the best answer it has. The final action is based on partial analysis.
- **Extracted Text Size (MB):** Assuming the transaction contains archives, the amount of text that is extracted from each file/sub-file for analysis.
- **Max Forensics Size (MB):** The maximum incident forensics size. Incidents do not include forensics beyond this limit. Transactions larger than this include just metadata.
- **Max Intercepted Size (MB):** The maximum content size submitted for analysis. Transactions larger than this are not sent to analysis.
- **Max Extracted Sub-Files (total in MB):** Assuming the transaction contains archives, the total amount of data to be extracted from these archives.

- **Max Extracted Sub-Files (count):** Assuming the transaction contains archives, the maximum number of sub-files that is extracted from these archives, including the archive level name.

F How Do I...

Here is a selection of quick tips for some of the most common tasks and procedures in the Websense Data Security system. The collection also supplies cross-references to more extensive explanations of the processes.

In this section, you can learn answers to these questions:

How do I...

Archive my incident data?

Select **Settings** > **Configuration** > **Archive** to view a list of current partitions and their status. If you want to save older partitions, you can archive them offline.To archive a partition:

1. Select the desired incident partition(s) in the Archiving screen.
2. Click **Archive** in the toolbar.
3. Review the list of partitions to be archived, adding comments if desired.
4. Click **OK** to continue.

The number of partition archives you can create depends on the size of the partition location.

For a deeper understanding of the archiving process (including restoring and deleting archives), see *Archiving a partition*, page 241.

Back up the system?

Related topics:

- *Configuring backup settings*, page 391
- *Monitoring backups*, page 391
- *Backup folder contents*, page 391
- *Restoring the system*, page 392

Backing up and restoring your Data Security data is a straightforward process that ensures that your critical information is secure and always accessible. The backup procedure is built into the Data Security Management Server, but disabled by default.

To perform a manual backup:

1. On the Data Security Management Server, open the Windows control panel and select **Scheduled Tasks**.
2. Right-click the “DSS Backup” task, and select **Run** or **Run Now**. Your data is backed up to the specified root folder (see *Configuring backup settings* below).

To create a backup schedule:

1. In the **Scheduled Tasks** window, double-click the “DSS Backup” task.
2. Select the **Schedule** tab.
3. Edit the schedule as required.
4. On the **General** tab or **Task** tab (depending on your operating system), select the **Enabled** check box.
5. Click **OK**.

All backups are “hot”—that is, they do not interfere with system operation. However, Websense advises that you schedule backups when the system isn’t under significant load. Each backup contains a complete snapshot of the system. The process collects needed information from other Data Security machines.

If for some reason a backup fails, refer to the log file **CPSBackup.log** stored in the Data Security installation directory.

Configuring backup settings

Most backup settings are configurable in the file, **BackupSettings.xml**. You can find this file in the directory where you installed Websense Data Security. This file includes the following parameters:

- **BackupPath -** a root folder into which all backups are written. Create the folder before running the task. The folder name cannot have a space in it. If the folder does not exist, or if it contains a space (for example: c:\back up\), the backup fails.

  Each backup process creates a new sub-folder inside that root folder. The name of each sub-folder is the timestamp when it was created.
- **BackupMax -** the maximum number of backups to store. When a backup process is complete, it checks whether the backup root folder contains more than the specified BackupMax directories, and if so, deletes the backups from the oldest to the newest until the BackupMax is reached.
- **BackupDomain, BackupUser, BackupPass -** in case BackupPath is a remote UNC path, and the Data Security administrative doesn't have write privileges to that path, use these fields to specify credentials to use for writing backups. Because the password is written in the clear in this file, using this field isn't recommended; instead Websense suggests granting the Data Security administrative account write-access to the backup location.

Monitoring backups

Every backup operation writes an entry in the windows event-log of TRITON - Data Security, and third-party tools such as Microsoft's SCOM and the open-source Zenoss can be used to monitor the backup process and create alerts and reports.

Backup folder contents

The backup folder contains a log file, which describes the circumstances of the backup process, and several sub-folders—each is a backup of a different component in the system:

- PreciseID_DB: the fingerprint repository
- MngDB: the TRITON - Data Security database (containing policies, incidents and configuration)
- Forensics_repository: the (encrypted) forensic incidents information
- Crawlers: information on the discovery and fingerprinting crawlers

The backup also contains additional information, either in sub-folders or directly in the backup folder. This information may include:

- Encryption keys (used by the endpoint encryption feature, and by the forensics repository)
- Your subscription file
- Your customized policy packages
- Other relevant information that completes a "snapshot" of the system

Restoring the system

You can activate the restore operation from the Data Security Management Server “Modify” wizard.

> **Important**
>
> Do not restore the backup into a machine that already exists in the backup topology—unless it is the management server itself. For example, if machine A is a master, and machine B is secondary to machine A, do not restore the backup of machine A into machine B.

To restore your system:

1. Make sure all Data Security modules—servers, agents, protectors—are registered with the Data Security Management Server and the system is operating normally.
2. On the Data Security Management Server, open the Windows control panel and select **Add/Remove Programs**.
3. Select Websense Data Security.
4. Click the **Change/Remove** button.
5. When asked if you want to add, remove, or modify Data Security, select **Modify**.
6. Click **Next** until you get to the **Restore Data from Backup** screen.
7. Select the **Load Data From Backup** check box and click the **Browse** button to locate the backup file.
8. Select the **Clear Forensics since last backup** check box if you want to use only the stored forensics from your backup file; this will remove all forensics gained since the last backup. (Leaving it unchecked means that your forensics data after the restore will include the backed-up forensics and the forensics added since that backup.)
9. Click **Next** until you get to the **Recreate Certificate Authority** screen.
10. Select the **Recreate Certificate Authority** check box, and enter a temporary password for restablishing secure communication with other components of the system. (This step is unnecessary, and can be skipped, if you are restoring a backup that was taken from the same machine and Data Security was not uninstalled since the backup file was created.)
11. Click **Next** until you begin the restore procedure.
    - During the restore process, a command-line window appears; it may remain for some time, but it disappears when the recovery is complete.
    - The restore operation completely erases all policies and data (and, if checked, forensics) of the current system, and replaces them with the backed-up data.
12. Complete the restore wizard.
13. To follow the restore activity, read the **DataRestore.log** file located in the backup folder (e.g., MM-DD-YYYY-HH-SS).

14. If you re-created the certificate authority for the management server:

    a. Re-register all the remote agents by running the installer (**WebsenseDataSecurity75.msi**) in Modify mode on the machines where the agents are installed.

    b. Re-register all protectors by logging into each protector as a root user and running the “wizard Securecomm” command.

    Refer to Chapter 3 of the *Data Security Deployment Guide* for more information on re-registering components.

15. Log onto TRITON - Data Security and select **Deploy**.

> ✓ **Note**
>
> If the backup system contains many policies, it may take a while to load the policies and deploy them.

Configure a policy?

Websense Data Security comes with a rich set of predefined policies that cover the data requirements for a variety of regulatory agencies. However, your company needs may mandate creating new policies or customizing predefined ones. After you create a regulatory policy using the first-time policy wizard, you may want to create custom policies as well.

To create a custom policy, do the following:

1. From the **Main** tab, select **Policy Management** > **Data Usage Policies** if you want to create a policy to govern data in motion across your network or on endpoint machines.

   or **Policy Management** > **Data Discovery Policies** if you want to create a policy responsible for discovering the location of sensitive data in your network.

2. In the toolbar, click **New** > **Policy**.
3. Complete the fields as follows:

Field	Description
Policy name	Enter a name for this policy.
Enabled	Select this check box to enable the policy in your organization. Leave it unchecked if you plan to enable it later. Policies can be deployed in an enabled or disabled state. Only enabled policies are applied across your organization.

Field	Description
Description	Optionally, provide a description of this policy.
Policy owners	By default, no policy owners are included in the policy. To define a policy owner(s), click **Edit**. In the resulting box, select the people who should receive notification in the event of a policy breach. Click the right-arrow to move them into the Selected List. These are known as *policy owners*. See *Selecting items to include or exclude in a policy*, page 47 for instructions on using the selector tool.

4. Click **OK**. The Create a Rule dialog box appears, because all policies must contain at least one rule.
5. Indicate whether you want to use express or advanced mode to create the rule. Express mode handles most of your needs.

Field	Description
Express mode	Select this mode if you want to accept the default rule properties for your data.
Advanced mode	Select this if you want to specify rule properties using a wizard.
I don’t want to create a rule now	Select this if you want to create a rule later. you can add one any time by highlighting a policy and clicking New Rule.

Proceed from the express/advanced mode decision to the policy-creation wizard, which will direct you through the completion of the process. See the explanations for the use of express or advanced mode, and the policy wizard at:

Using express mode, page 51

Using advanced mode, page 53

Rule Wizard - General, page 53

Create a custom block message?

For HTTP/FTP via Websense Content Gateway:

1. From the TRITON - Data Security user interface, select **Settings** > **Configuration** > **System Modules**.
2. Select the Content Gateway module.
3. Select the **Advanced** tab.
4. Set **Mode** to **Blocking.**
5. Click **Custom message** and browse to the message you want to display when a violation occurs.
6. Click **OK** to save your changes.

7. Click **Deploy** to deploy your settings.

For HTTP via the protector:

Change the code in /opt/pa/conf/http_block_notification.html

For ICAP via the protector:

Change the code in /opt/pa/conf/spicer/icap-pa_block.markup.

Once this is done, restart the protector services with the **service pama restart** command and the new block page code will display.

Define an exception?

Most rules have exceptions. There are a few ways to add an exception to a rule. On the **Main** tab under Policy Management, look at your policies' tree view.

click a rule and select **New** > **Exception** from the pull-down menu.

Highlight a rule and select **New** > **Exception** from the toolbar.

click an exception and select **New** > **Exception Above** or **Exception Below**.

This inserts the exception in an order of priority relative to others. The exception begins empty—you must select the fields to edit. The other fields retain the same data as the rule. You can review the process for using the exception wizard and obtain more information on adding (and rearranging) exceptions by seeing *Adding a new exception*, page 63.

Filter incidents?

You can filter incidents in a report by editing report filters or applying column filters.

Editing report filters

To change the filters that are applied to this report, select **Manage Report** > **Edit Filter**.

1. On the **General** tab, change the name or description of the report as desired.
2. Select whether you want all administrators to have access to the report, or just the current administrator.
3. Select the date range you want represented on the report. You can select to view incidents from the last x days, from a date range such as this week or last month, or from an exact date range. Also specify the time of day to include.
4. On the **Filter** tab, select the filter(s) to apply to the report. When you select a filter to apply, options appear in the Filter Properties pane.

5. For each filter you select, select filter properties. For example, if you select the Action filter, indicate which actions you want to include in the report. If you select **Channel**, select which channels to include.
6. Click **OK** when you're done.
7. To save the report for later use, select **Manage Report > Save As**.

Applying column filters

The incidents list is a table displaying all data usage or data discovery incidents. By default, incidents are sorted by their event time, but you can sort them (ascending or descending) by any of the columns in the table. You can also group by and filter by columns.

To filter incidents by columns in the incident list:

1. Click the down arrow button in a column header. A drop menu with 5 options appears. Different columns display different options.
2. Select **Filter by column**. A pop-up box appears. You can filter the column according to specific words or according to excluded words.
3. Select one of the following options in the Must field:

   Be equal to - Enter a specific word in the text field that you want included in the column and click **OK**.

   Be empty - Enter a specific word in the text field that you want excluded in the column and click **OK**.

   The results are displayed in the column with or without the specific words in the column.

   * Note: When a column is filtered, the header arrow turns blue.
4. To clear a column filter, click the down arrow button in a column header and select **Clear Column's Filter**.

Fingerprint data?

To fingerprint files and directories:

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **PreciseID Fingerprinting - Files and Directories**.
3. Click **New** > **File System Fingerprinting** or **New** > **SharePoint Fingerprinting** from the menu bar.
4. You'll see the PreciseID Fingerprinting wizard, which will guide you through the process.
5. When finished with the wizard, click **Run** to perform the scan.
6. Add the fingerprint classifier to a rule/policy when prompted.

For more information fingerprinting files and directories, see *PreciseID Fingerprinting - files & directories*, page 84.

To fingerprint a database or CSV file:

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **PreciseID Fingerprinting - Database Records**.
3. Click **New** > **Database Table Fingerprinting** or **New** > **CSV File Fingerprinting** from the menu bar.
4. You'll see the PreciseID Fingerprinting wizard, which will guide you through the process.
5. When finished with the wizard, click **Run** to perform the scan.
6. Add the fingerprint classifier to a rule/policy when prompted.

For more information and best-practices advice on fingerprinting database records, see *PreciseID Fingerprinting - database records*, page 89.

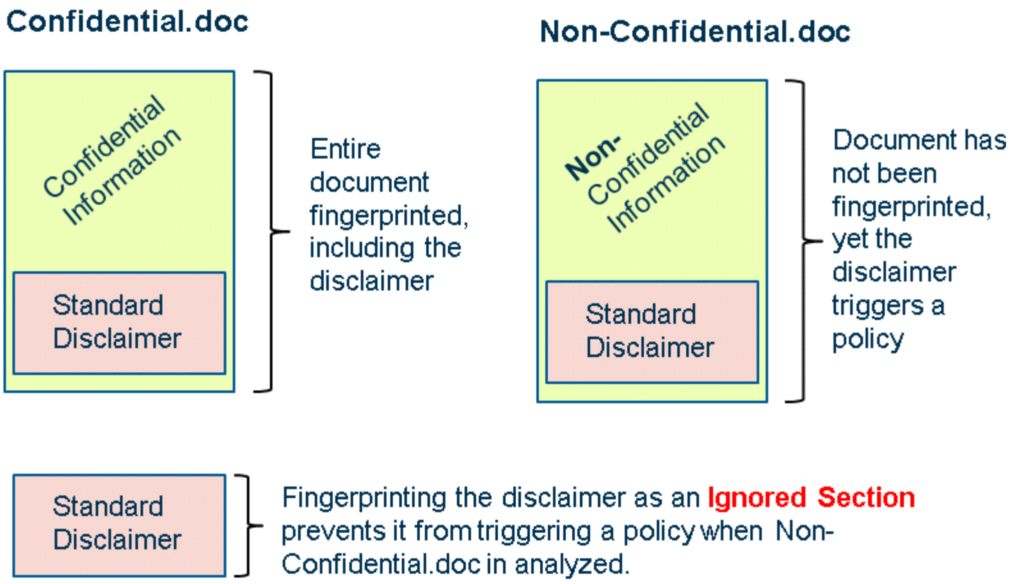
Ignore sections of my document when fingerprinting?

For file system or SharePoint fingerprints, create a separate document with the text to ignore. For example, if you want to ignore material with your company's copyright statement or a standard disclaimer, copy that statement and paste it into a new document. Now create a classifier with the fingerprinting mode "Ignored Section".

1. Select **Main** > **Content Classifiers** > **PreciseID Fingerprinting - Files & Directories**.
2. Click **New**, then choose the type of fingerprint to create: file system or SharePoint.
3. On the General tab of the wizard, select **Ignored Section** for the Fingerprinting Mode.
4. On the **Scanned Files** or **Scanned Documents** page, click **Edit**.
5. In the left pane of the selector, highlight the file you created.
6. Click the right arrow to move the file into the Include list.
7. Click **OK**.
8. Continue through the wizard, and click **Finish** when done.
9. Run the fingerprint scan.

Fingerprinting the copyright or disclaimer as an ignored section prevents it from triggering a policy when a non-confidential document is analyzed. If this fingerprinted data later appears in a transaction, Data Security detects it and knows to ignore this section. Ignored sections apply to all policies.

If you did not create an ignored section, and instead fingerprint a confidential document containing a disclaimer or copyright, then any time a document contained that disclaimer or copyright an incident would be triggered, creating many unintended matches.


Confidential.doc
Confidential Information
Standard Disclaimer
Entire document fingerprinted, including the disclaimer
Non-Confidential.doc
Non-Confidential Information
Standard Disclaimer
Document has not been fingerprinted, yet the disclaimer triggers a policy
Standard Disclaimer
Fingerprinting the disclaimer as an Ignored Section prevents it from triggering a policy when Non-Confidential.doc in analyzed.

Fingerprint specific field combinations in a database table?

To fingerprint specific field combinations, you must first create a fingerprint classifier for the database table:

1. Click **Main** > **Policy Management** > **Content Classifiers**.
2. Select **PreciseID Fingerprinting - Database Records**.
3. Click **New** from the menu bar, then choose **Database Table Fingerprinting**.
4. Work through the wizard as described in *Creating a PreciseID database-record fingerprint classifier*, page 95. On the Field Selection page, select **Select fields from a table**, then select the table name and the field combination you want to fingerprint.
5. Continue through the wizard, and click **Finish** when done.
6. Run the fingerprint scan.

You then add the fingerprint classifier you created to a rule. If you want, you can add the same classifier more than once, selecting a different combination of fields and different thresholds to match against.

1. Click **Main** > **Policy Management** > **Data Usage Policies**.
2. Select the rule where you want to add the classifiers, then click **Edit**.
3. Select **Condition** from the rule properties.

4. Click **Add**, then choose **PreciseID Fingerprinting - Database Records** from the drop-down list.
5. Select the content classifier you want to add, define the field combination and threshold you want to use, then click **OK**.
6. If you want to add the same classifier again with a different field combination and threshold, repeat steps 4 and 5.
7. Set up the condition relations for your classifiers using the **And**, **Or**, and **Customized** radio buttons. For more information on setting up conditions, see *Rule Wizard - Condition*, page 54.

Import/export the Oracle database?

To export the Oracle database to a specified output file, enter:

```
Cscript.exe OraImport.vbs OutPutFileExample: Cscript.exe
OraExport.vbs c:\IncidentsData.dmp
```

To import data from a specified input file, you must first recreate the user for that database. The **OraImport.vbs** imports the specified file with the incidents data that was created by OraExport. The data is consistent with the original schema. Normally you should use the SA credentials.

Example:

```
Cscript.exe RecreateUser.vbs cscript OraImport.vbs
c:\IncidentsData.dmp SA
```

Mitigate false positives in pattern or dictionary phrases?

One way of mitigating false positives in a pattern or dictionary phrase is to exclude certain values that falsely match it. When defining the classifier, you can define a *Pattern to exclude* listing words or phrases that are exceptions to the rule (search for all Social Security numbers except these numbers that look like Social Security numbers but are not).

You can also add a *List of strings to exclude* listing words or phrases that, when found in combination with the pattern or phrase, affect whether or not the content is considered suspicious. These fields are available for both PreciseID Pattern classifiers and dictionary classifiers.

Move from monitor to protect?

Websense recommends that you initially set your policy to apply to all sources and destinations of data with a permissive action. Later, you can permit or block certain sources and destinations and apply more restrictive actions.

You must have a subscription to Websense Data Protect to move from monitoring to enforcing.

If you are using the protector to block SMTP or HTTP traffic, it must configured inline.

To block SMTP traffic with the protector:

1. Go to **System Modules** and select the protector.
2. In the Edit Protector window, select the **Services** tab, and double-click the SMTP service.
3. In the Edit SMTP Service window, under the General tab, choose **Mail Transfer Agent (MTA)** in the Mode drop-down menu.
4. Select the **Mail Transfer Agent (MTA)** tab, and in the drop-down menu under Operation Mode, select **Blocking**.
5. You can adjust various options from there. Click **OK** to save your changes.

To block HTTP traffic:

1. Go to **System Modules** and select the protector,
2. In the Edit Protector window, select the **Services** tab, and double-click the HTTP service.
3. In the Edit HTTP Service window, under the Advanced tab, choose **Blocking** in the Operation mode drop-down menu.
4. You can adjust various options from there. Click **OK** to save your changes.

Action plans

Action plans can also be configured to block incidents that contravene policy. Select **Main** > **Policy Management** > **Resources** >**Action Plans** to configure action plans.

Click the pencil icon to edit an action plan. You can change the action for each channel if desired (quarantine for SMTP, block for HTTP). Click the paper icon to create a new action plan.

See *Action Plans*, page 112 for more information.

Perform discovery?

To perform discovery:

1. Create a data discovery policy. (See *Creating a data discovery policy*, page 124 for instructions.)
2. Select **Main** > **Policy Management** > **Data Discovery Tasks**.
3. Select **Network Tasks** or **Endpoint Tasks**.
4. Click **New** on the toolbar. If you selected Network Tasks, select the type of discovery you want to perform.

5. Complete the fields on the screen and click **Next** to proceed through a wizard.
6. For details on each screen, see the sections below:
   - *Performing file system discovery*, page 126
   - *Performing SharePoint discovery*, page 127
   - *Performing database discovery*, page 128
   - *Performing Exchange discovery*, page 129
   - *Performing endpoint discovery*, page 130
7. Deploy your changes by clicking **Yes** when prompted.
8. Discovery will take place at the time and day you scheduled in step 5c. To start it immediately, click **Switch to Mode > Manual**, then click **Start > Full Scan**. A message indicates when the scan finishes.
9. To view and respond to discovery results, click **Main** > **Incidents & Reports** > **Data Discovery**. See *Viewing the incident list*, page 175 for information on reading these screens.

Permanently delete incidents?

You can delete discovery incidents, but you cannot delete data usage incidents.

To delete a single discovery incident, locate the incident in question and select it by clicking the check box on the left. From the toolbar, select **Workflow** > **Delete** > **Delete Selected Incidents**.

To delete multiple incidents, use the display and column filters so that only the incidents you desire to delete are displayed. Select all displayed incidents. Click the red X in the tool bar and select **Delete Selected Incidents**.

To delete all discovery incidents, select **Workflow > Delete > Delete ALL Discovery Incidents**.

G Glossary

A

Analysis

The process that the Data Security system uses to examine data to determine whether it contains protected content.

Assigned/unassigned incident

Incidents can be tracked through the system by administrators. To give a single administrator the responsibility to handle the incident, you can assign the incident to that administrator. Incidents that can be handled by any administrator are considered **unassigned**.

Authorization

The instruction to override security policy and send blocked email to the intended recipient. This can be performed by a security officer or by a content owner.

Authorization Code

The Data Security-generated code contained in a Block email notification. When a reply is sent to the Block notification, the Authorization Code releases the blocked transmission.

Authorized Recipient

A user who is allowed to receive protected content.

B

Blocking

The prevention of data containing protected information from being sent to an unauthorized recipient.

C

Content Group

An empty shell to which you later assign directories containing classified information of a certain type. Each directory within a Content Group can be assigned a security level that restricts its contents to users with matching or higher security levels.

Content Owner

A Content Owner can define and modify a file’s distribution security policy. Content Owners can override security policy and authorize the distribution of a blocked transmission to the intended recipient.

Crawler

The Crawler is the agent that scans your documents looking for sensitive data. You can have several in your network if you are managing many documents.

D

Data Security Administrator

A user who manages and maintains the data security system.

Data Security Database

A Data Security component that stores the system configuration, settings, and roles that determine the behavior of the application; it also stores information about traffic transmitted through the system.

Data Security File Fingerprinter

A Data Security component that scans specified folders and submits files for fingerprinting to the Data Security DMS API.

Data Security Fingerprint Server

A Data Security component that analyzes corporate file directories at predefined intervals and fingerprints files.

Data Security Management Server

The Management Server is the Websense Data Security component that includes all core technology and Websense fingerprinting servers, policy servers, and patented data loss prevention technology.

Data Security MS Exchange Agent

A Data Security component that receives all internal email from the Microsoft Exchange mail server and forwards it to the Data Security Policy Engine. The Data Security Exchange agent then receives the analyzed email back from the Data Security Policy Engine and places it in the recipient’s mailbox.

Data Security Server

The server that controls all aspects of the Data Security software.

Data Security SMTP Agent

A Data Security component that receives all outbound email from the mail server and forwards it to the Websense Data Security Policy Engine. The Websense Data Security SMTP agent then receives the analyzed email back from the Websense Data Security Policy Engine and forwards it to the mail gateway.

E

Event

An event is any transaction that traverses the Data Security system. Not all events are stopped by the Data Security sniffer and queued for analysis—for that to happen, something has to look suspicious, meaning that something in the event seems to match with a Policy rule.

- **Unmatched events** are events that pass through the system transparently, because they raise no suspicion.
- **Policy matches** are events that are analyzed as they traverse the system, because something in the transaction is suspicious according to the policies. Policy matches are then either deemed **authorized incidents**—events that seemed to match a policy but are in fact allowed—or **incidents**, which are policy violations.

Exchange Agent

See Data Security MS Exchange Mail agent (Internal).

External User

A user who is outside the organization or domain.

F

File System Directories

Registered directories on the corporate file server that contain files with classified content.

File Type

A data format, such as .doc, .pdf, or .xls.

Fingerprinting

See Registering.

Forensics Repository

The forensics repository contains complete information about your original transactions. In SMTP, for instance, it stores the original email message that was sent. For other channels, the system translates transactions into EML.

To configure the forensics repository, select it on the System Modules screen.

I

Ignored Incident

Incidents that are set as Ignored Incidents. Often files that are determined not to be violations or incidents (files or attachments) that are not malicious, can be set to be ignored. These incidents can then be filtered in or out using the main and quick filters.

Often, it is useful to set an incident as “ignored” when an incident was determined not to be a violation, (it looks like a violation but is not). Understanding ignored incidents can assist you in fine-tuning your policies to avoid blocking traffic unnecessarily. By default, the data presented in TRITON - Data Security does not include incidents marked as ignored. Refer to “Filtering Incidents” to modify this setting.

Incident

An Incident is a transaction that violates a policy.

Assigned/Unassigned Incident: Incidents can be tracked through the system by administrators. To give a single administrator the responsibility to handle the incident, assign the incident to a single administrator. Unassigned Incidents are those that have not been assigned and can therefore be handled by any administrator who has access to the incident.

Incident Database

The incident database saves basic information about incidents plus additional information that helps you analyze the data, such as: source, destination, the resolved source/destination host name, breach information, analyzed by, detected by, and assigned to.

The incident database is part of the main Oracle management database.

Information Lifecycle

The changes (over time) to the importance level of information, from its most sensitive level at creation to its general distribution.

Internal MS Exchange Mail Agent

See Data Security MS Exchange Mail agent (Internal).

SA

Microsoft’s Internet Security and Acceleration server is a combination of two products: a proxy server and a firewall. Data Security uses the proxy part of the package.

ISA Agent

A Websense Data Security component that receives all Web connections from the network and forwards them to the Websense Data Security Policy Engine. The Websense Data Security ISA Agent then receives the analyzed information back from the Websense Data Security Policy Engine and forwards it to the recipients on the Web.

L

LDAP

Lightweight Directory Access Protocol is the protocol standard over TCP/IP that is used by email clients to look up contact information. Websense Data Security uses LDAP to automatically add users and groups to the data security database.

M

MAPI

The protocol that sends email to recipients inside an organization/domain.

Matching Keyword

A predefined text string that must be protected; its presence in a document indicates that the document contains confidential information.

N

Notification

An email alert sent to the Security Officers and Content Owners, indicating that the information was addressed to an unauthorized recipient.

O

Owner

See Content Owner.

P

Permissions

Permissions define what a user is authorized to perform within the Data Security structure.

Policy

Data security can be set to include multiple policies. A policy is a list of criteria to be searched for over your channels. These criteria are set with a certain rule which defines what the Data Security does when it comes across a transmission that meets the designated criteria.

Policy Category

Websense Data Security can be set to include multiple policies. These policies are grouped together to create policy categories.

Policy Category Group

Multiple policy categories can be grouped together to form policy category groups. These groups are then assigned to specific administrators for incident management and monitoring purposes. Often a policy category group reflects the corporate department associated with these events, such as Finance or Marketing. For example, the policy categories Intellectual Property, Malicious Concealment, and Source Code may be combined to form a policy category group called Technology. This group can then be assigned to administrators who are the VP of R&D and the CTO. These individuals would then be notified of violations of these policies and would be able to handle and track these incidents.

PreciseID File Fingerprints

Information that is protected by Websense Data Security. The information will be recognized even after the original file has been deleted from the corporate file server.

R

Registering

The process of identifying a unique set of characteristics for a document’s contents. Websense Data Security uses registering to uniquely identify classified content.

Roles

Security profiles that can be applied to several users without having to define security details for each user.

S

Security Level

A label, such as Top Secret, that represents a degree of confidentiality. Both users and classified content are assigned Security Levels. Users with a specific Security Level can only receive information classified with the same or lower Security Level.

Security Officer

A user who defines Websense Data Security security policies, and monitors security policy distribution within the organization. The Security Officer can override security policy and authorize the distribution of a blocked transmission to the intended recipient.

Security Policy

The policy within an organization that defines which classified information can be distributed to which recipients.

SMTP

The protocol used for sending email to recipients outside the organization.

SMTP Agent

A Websense Data Security agent that monitors SMTP traffic.

System modules

These are the various components of Websense data security solutions. They are either hardware-based physical devices, like the protector; software components, like TRITON - Data Security and SMTP agent; or virtual components like channels and services.

T

Traffic

The transmission of email messages sent through the electronic mail system or uploaded to the Internet.

TRITON - Data Security

The graphical user interface that enables the security officer to manage the Data Security system, define and monitor the distribution of security policies, and view reports.

TRITON Unified Security Center

A central management console that provides access to Websense data, Web, and email security modules. A system administrator can define and monitor the distribution of security policies, and view reports for all 3 modules from one location.

U

Unmatched Events

Unmatched Events are events that pass through the system transparently because they raise no suspicion.

Urgency

The incident's urgency setting is a measure of how important it is to the corporation that this incident is handled. The urgency of an incident is automatically decided by Websense Data Security. This calculation takes both the sensitivity of the incident and the number of matched violations into account.

For example, if content triggers a violation because it includes 400 credit card numbers, and the credit card policy was set to medium sensitivity, then the urgency is set to critical due to the large number of violations (400) and the sensitivity (medium). This setting provides you with a relative measure for how urgent it is for someone to deal with this incident.

Users

The personnel within an organization who can distribute and receive information.

V

Views

Views are views into the incident database with filters applied. Several built-in views are provided. The most common are displayed on the main Incidents & Reports page. Views are very much like reports; they're graphical and contain colorful executive charts.

Index