1 Web DLP Quick Start

Websense Data Security enables you to control how and where users upload or post sensitive data over HTTP or HTTPS connections.

The Web Security manager is automatically configured to work with the Data Security manager. The Web Security module registers with the Data Security Management Server when you install it.

> **Important**
>
> You must click **Deploy** in the Data Security manager to complete the registration process.

A quick-start web data loss prevention (DLP) policy is provided.You just need to configure it.

To get started with your Web DLP policy

1. Define user directories for Data Security users and other policy resources such as devices and networks. (See *Configuring user directory server settings*, page 2.)
2. Set up email properties for alerts (See.*Setting up email properties*, page 3.)
3. Select and enable the web attributes to monitor—for example uploaded file type. Configure properties for those attributes. When the settings you configure are matched, the policy is triggered. See *Configuring web attributes*, page 4 for instructions on completing the fields.
4. Specify specific websites where you do *not* want your data sent. See *Selecting web destinations*, page 7 for instructions.
5. Identify an owner for the policy. See *Defining policy owners*, page 10 for instructions.
6. Deploy your settings. (See *Deploying your settings*, page 10.)

> **Note**
>
> You can’t delete or rename your web policy, but you can enable or disable its attributes.

Configuring user directory server settings

To resolve user details during analysis and enhance the details displayed in reporting, you need to first configure user directory server settings.

In the TRITON Console, define the LDAP user directory to use *when adding and authenticating TRITON administrators* with network accounts. (Select **TRITON Settings** from the TRITON toolbar, then select **User Directories**.)

On the Data Security tab, you define the user directory to use *for Data Security users and other policy resources* such as devices and networks.

1. Select **Settings** > **General** > **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.
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 distinguished name	Enter a user name that has access to the directory server.
Password	Enter the password for this user name.
Root naming context	Optionally, enter the root naming context that Websense Data Security should use to search for user information. If you supply a value, it must be a valid context in your domain. If the **Root naming context** field is left blank, Data Security begins searching at the top level of the directory service.
Use SSL encryption	Select this box if you want to connect to the directory server using Secure Sockets Layer (SSL) encryption.
Follow referrals	Select **Follow referrals** 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.
Test Connection	Click this button to test your connection to the user-directory server.
Directory usage	
Get user attributes	Select this box if you want to retrieve user attributes from the directory server.

Field	Description
Attributes to retrieve	Enter the user attributes that you want the Data Security manager to collect for all users (comma separated).
Photo attributes to retrieve	Enter the valid photo attributes, thumbnailPhoto (default), to display a photo of the user (comma separated). ◆ If you do not want to display a photo of the user, leave this field blank. ◆ If a photo does not exist for the user, an empty image displays.
Sample email address	Enter a valid email address with which you can perform a test.
Test Attributes	Click **Test Attributes** to retrieve user information, such as the user's attributes and email address you supplied.

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 email properties

Set up the email properties, such as SMTP mail server, to be used for system alerts.

1. Select **Settings** > **General** > **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, scheduled tasks, and email workflow. The settings you use here apply to the other cases, and if you change the settings for one, it affects the others.

Configuring web attributes

Configure the attributes that you want to monitor on web channels.

1. In the Data Security manager, select **Main** > **Policy Management** > **DLP Policies** > **Web DLP Policy**.
2. On the Attributes tab, select one or more web attributes to include in the policy, then define parameters for those attributes in the right pane. When Data Security detects a match for an attribute, it triggers the policy. (Refer to the following table for a description of each attribute.)
    a. If you want to send notifications when there is a violation of a particular attribute setting, select the **Send the following notification:** check box. You can configure who receives the notifications by clicking the name of the notification, “Web policy violation.” Click this option to define the mail server, email subject, and message body, as well as other required properties. Policy owners receive notifications by default.

b. For each attribute, indicate how severe a breach would be (low, medium, or high severity), and what action should be taken if a breach is detected. The default severity levels and available actions are shown below for each attribute.

Field	Description
Post size	Disabled by default. Select the size of web posts to monitor. For example, choose 100 KB if you want Data Security to analyze posts equal to or exceeding 100 KB and enforce the policy, but you're not concerned about posts smaller than 100 KB, even if there is a match. The default is 10 KB. Default severity: **low**. Available actions: **block** (default), **permit**.
Regulatory & compliance	Enabled by default. Select the regulatory and compliance rules you need to enforce. These are applied to the regions you selected with the regulatory & compliance option. - Personally Identifiable Information (PII) - Protected Health Information (PHI) - Payment Card Industry (PCI DSS) If you have not selected regions, an error pops up. Click **Select regions** to fix this. Once you've selected a category, click its name to view or edit the specific policies to enforce. Applying only the policies you need improves performance and reduces resource consumption. Select a sensitivity for each policy. - **Wide** is highly sensitive and errs on the restrictive side; it detects more data than the other levels. It is more likely to produce a false positive (unintended match) than a false negative (content that is not detected). - **Default** balances the number of false positives and false negatives and is recommended for most customers. - **Narrow** is the least restrictive. It is more likely to let content through than to produce an unintended match. For best practice, use this level when you first start using the block action. You might also use it if the system is detecting too many false positives. Default severity: **high**. Available actions: **block** (default), **permit**.

Field	Description
Data theft	Disabled by default. Data Security protects against content being posted to the web after your computer is infected. This complements the Web Security module which protects against infected content downloaded from the web. Select the type of data to search for in outbound transactions. When sent outside your network, this data can indicate a serious vulnerability. ◆ **Malware** - Identifies transactions that are suspected to be malicious, based on analysis of traffic of known infected machines. ◆ **Encrypted files - unknown format -** Searches for encrypted data of an unknown format, based on advanced pattern and statistical analysis of the data. ◆ **Encrypted files -** Searches for outbound transactions comprising known encrypted file formats, such as password-protected Microsoft Word files. ◆ **Password files -** Searches for outbound password files, such as a SAM database. ◆ **Common password information -** Searches for outbound password information in plain text by looking for common password patterns and using various heuristics. ◆ **Credit card magnetic strips -** Searches for outbound electronic data from credit card strips. ◆ **Number of posts -** Searches for data being posted numerous times in a designated period. ◆ **Cumulative encryption -** Searches for the number of transactions comprising encrypted data over time. Select a sensitivity for each policy. ◆ **Wide** is highly sensitive and errs on the restrictive side; it detects more data than the other levels. It is more likely to produce a false positive (unintended match) than a false negative (content that is not detected). ◆ **Default** balances the number of false positives and false negatives and is recommended for most customers. ◆ **Narrow** is the least restrictive. It is more likely to let content through than to produce an unintended match. For best practice, use this level when you first start using the block action. You might also use it if the system is detecting too many false positives. **Note:** The number of policies and sensitivity you select affects performance. Default severity: **high**. Available actions: **block** (default), **permit**.

Field	Description
Name of uploaded file	Disabled by default. One by one, enter the names of the exact files that should be monitored when they're posted or uploaded to the web. Include the filename and extension. Click **Add** after each entry. For example, add the file named **confidential.docx**. When that file is being posted, Data Security will detect it and either permit or block the post. Data Security can detect files even when they've been compressed into an archive, such as a .zip file. Default severity: **low**. Available actions: **block** (default), **permit**.
Type of uploaded file	Disabled by default. Click **Add** to specify the types of files that should be monitored when posted or uploaded to the web, for example Microsoft Excel files. From the resulting dialog box, select the type or types of files to monitor. If there are more file types than can appear on the page, you can sort columns or enter search criteria for find the type of file you want. If the file type does not exist, specify exact files of this type using the **Name of uploaded file** attribute instead. Default severity: **low**. Available actions: **block** (default), **permit**.
Patterns & phrases	Enabled by default. Click **Add** to define key phrases or regular expression (RegEx) patterns that should be monitored. On the resulting dialog box, enter the precise phrase (for example "Internal Only") or RegEx pattern (for example ~ m/H.?e/) to include. Select how many phrase matches must be made for the policy to trigger. The default number of matches is 1. Default severity: **medium**. Available actions: **block** (default), **permit**. **Note:** Although you do not define whether to search only for unique strings, the system will use the following defaults: Key phrase: non-unique - all matches will be reported. Regular expression: unique - only unique matches will be reported as triggered values.

Selecting web destinations

If desired, you can define specify websites where you do not want data posted, for example, known malware sites.

1. Select the Destinations tab.

2. Select one or more websites to include in the policy. When Data Security detects that someone is posting sensitive data to those websites, it triggers the policy.

Field	Description
Destination Sites	
Any website	Select this option if you do not want sensitive data posted or uploaded to any website, without exception.

Field	Description
Websites that belong to the selected categories	Select this option to prevent sensitive data from being posted or uploaded to known or potentially hazardous websites, but not to all websites. You must have Websense Linking Service installed and running to monitor selected categories. The service must also be enabled (**Settings > General > System > URL Categories and User Names**) and the connection to the Linking Service machine must be working, or this option is grayed out. Expand a category to select or deselect specific site categories. ◆ *Identified malware sites* are websites that have been identified as containing malicious software, such as software designed to infiltrate a computer system without the owner's consent. Identified malware sites include: • Botnets • Keyloggers • Malicious embedded Link • Malicious embedded iFrame • Malicious websites • Phishing and other frauds • Spyware • Emerging Exploits ◆ *Suspected malware sites* contain potentially malicious or undesired content These include: • Potentially unwanted software • Suspicious embedded link • Potentially damaging content • Elevated exposure • Illegal or questionable ◆ *Data misuse sites* are websites prone to misuse, intentional or not, by users. For example, users may post sensitive data to a message board or blog. Suspected data misuse sites include: • Peer-to-peer file sharing • Personal network storage and backup • Instant messaging • Message boards and forums • Hosted business applications • Web collaboration • Web chat • General email • Organizational email • Text and media messaging • Blogs and personal sites • Social networking • Social networking and personal sites • Uncategorized

Field	Description
Trusted Domains	
Enable trusted domains	Select this check box if you do not want certain network domains to be monitored, then click **Edit** to select the trusted domains. Websense Data Security does not enforce trusted domains. This means they can receive any type of sensitive information via HTTP, HTTPS, or other web channels.

Defining policy owners

Policy owners can modify a policy and, if configured, receive notifications of breaches. Notifications must be enabled in one or more of the policy's attributes for notifications to be sent.

To define an owner or owners for this Web DLP policy:

1. Click the Policy Owners tab.
2. Click **Edit**.
3. Select one or more owners from the resulting box.
4. Click **OK**.

If you would like notifications to be sent to policy owners:

1. Select **Main** > **Policy Management** > **Resources**.
2. Click **Notifications** in the Remediation section of the page.
3. Select an existing notification or click **New** to create a new one.
4. Under Recipients, select **Additional email addresses**.
5. Click the right arrow then select the variable, %Policy Owners%.
6. Click **OK**.

Deploying your settings

The settings you configured in this chapter must be deployed to the Web Security module and other system components to begin monitoring your web channels. To deploy settings:

1. Click **OK** on the Web DLP policy page.
2. Click **Deploy** in the Data Security manager toolbar.

Your Web DLP policy is now functioning!